Department of Homeland Security
Information Analysis and Infrastructure Protection Directorate

CyberNotes

Issue #2003-06 *March 24, 2003*

Effective March 1st the National Infrastructure Protection Center officially moved into the new Department of Homeland Security under the Information Analysis and Infrastructure Protection (IAIP) Directorate.

CyberNotes is published every two weeks by the Department of Homeland Security/National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, Room 5905, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between March 2 and March 21, 2003. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
3Com[1]	Multiple	SuperStack 3 Firewall	A vulnerability exists in the content filtering features because fragmented packets are not reassembled when a HTTP request is checked against the list of restricted sites and phrases, which could let a remote malicious user bypass the filtering mechanism and obtain unauthorized access.	No workaround or patch available at time of publishing.	SuperStack 3 Firewall Content Filter Bypassing	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Andries Brouwer[2]	Unix	man 1.5 k	A vulnerability exits in the man program because some types of input are not handled properly, which could let a malicious user execute arbitrary commands.	Upgrade available at: ftp://ftp.win.tue.nl/pub/linux-local/utils/man/man-1.5l.tar.gz	Man Program Unsafe Return Value Command Execution	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Apache Software Foundation[3] ***Hewlett Packard releases patch[4]***	**Unix**	**Tomcat 3.0- 3.3.1**	**Multiple vulnerabilities exist: a directory/file disclosure vulnerability exists due to improper handling of null bytes and backslash characters in requests for web resources, which could let a remote malicious user obtain sensitive information; a file disclosure vulnerability exists because it is possible to create a malicious 'web.xml' file, which could let a malicious user obtain sensitive information; and a Cross-Site Scripting vulnerability exists in sample web applications, which could let a remote malicious user execute arbitrary code.**	**This issue will reportedly be addressed by the vendor in Tomcat 3.3.2.** **Debian:** **http://security.debian.org/pool/updates/contrib/t/tomcat/** **Apache (corrects the directory/file disclosure vulnerabilities):** **http://jakarta.apache.org/builds/jakarta-tomcat/release/v3.3.1a/** ***Hewlett Packard:*** **http://www.software.hp.com/**	**Tomcat Multiple Vulnerabilities** **CVE Names: CAN-2003-0042, CAN-2003-0043, CAN-2003-0044**	**Medium/ High** **(High if arbitrary code can be executed)**	**Bug discussed in newsgroups and websites.**
Basit[5]	Windows, Unix	Basit 1.0	Cross-Site Scripting vulnerabilities exists in the submit and search modules due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	Basit Submit Module & Search Module Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploits have been published.

[1] Bugtraq, March 4, 2003.
[2] Sorcerer Update Advisory, SORCERER2003-03-06-1, March 11, 2003.
[3] Debian Security Advisory, DSA 246-1, January 29, 2003.
[4] Hewlett-Packard Company Security Bulletin, HPSBUX0303-249, March 18, 2003.
[5] SecurityFocus, March 19, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
BEA Systems, Inc.[6]	Windows 98/NT 4.0/2000, XP, Unix	Weblogic Server 6.0, 6.0 SP1&2, 6.1, 6.1 SP1-SP4, 7.0, 7.0 SP1&2	Multiple vulnerabilities exist: an input validation vulnerability exists in the web management interface internal servlet, which could let an unauthorized malicious user execute arbitrary code; a vulnerability exists in several undocumented applications that are normally used for data replication between servers and supporting application deployment, which could let a malicious user obtain unauthorized access; a vulnerability exists because a component that implements session persistence is redistributed without a server reboot, which could let a malicious user obtain unauthorized access; and a Denial of Service vulnerability exists in the JNDI tree because the performance of some unauthorized functions are allowed.	Patches available at: ftp://ftpna.beasys.com/pub/releases/security/	WebLogic Multiple Vulnerabilities	Low/ Medium/ **High** **(Low if a DoS, Medium if unauth-orized access can be obtained, and High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required.
BitchX[7]	Windows, Unix	IRC Client 1.0 c19	Multiple vulnerabilities exist: a vulnerability exists when an excessively long hostname is supplied, which could let a remote malicious user execute arbitrary code; a vulnerability in Send_CTCP() when handling server-supplied data, which could let a remote malicious user execute arbitrary commands; a buffer overflow vulnerability exists in cannot_join_channel() when handling server-supplied data, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary commands; and a buffer overflow vulnerability exists in BX_compress_ modes()when an excessive amount of data is supplied, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	BitchX Multiple Vulnerabilities	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.

[6] BEA Systems Security Advisory, BEA03-28.00, March 18, 2003.
[7] Bugtraq, March 13, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Broadpool [8]	Windows, Unix	Siteframe 2.2.4	Several vulnerabilities exist: a Cross-Site Scripting vulnerability exits in the 'search.php' script due to insufficient filtering of user-supplied URI parameters, which could let a remote malicious user execute arbitrary HTML and script code; and an information disclosure vulnerability exists when certain download request are handled, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Siteframe search.php Cross-Site Scripting & Information Disclosure	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploits have been published.
Clearswift Limited[9]	Windows NT 4.0/2000	Mail Sweeper 4.0	A vulnerability exists because certain malformed MIME e-mail message attachments are not properly processed, which could let a remote malicious user bypass mail attachment filtering mechanisms.	Updated script utility available at: http://www.clearswift.com/support/threatlab/vbstool.asp	MailSweeper Attachment Filter Bypass CVE Name: CAN-2003-0121	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Cyber-Cats [10]	Windows, Unix	Chitchat	A vulnerability exists in the PHP Message Board/ Guestbook because access to files on the local system has insufficient limitations, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Chitchat PHP Message Board/ Guestbook File Limitations	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
DBTools [11]	Windows	DB Manager Profes-sional 2.0.1	A vulnerability exists in the 'catalog.mdb' file because sensitive information is stored in plaintext, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	DBManager Professional Information Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
DCP-Portal[12]	Unix	DCP-Portal 5.3.1	Cross-Site Scripting vulnerabilities exist in the 'search.php' and 'calendar.php' scripts due to insufficient sanitization of user-supplied URI parameters, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	DCP-Portal 'Search.php' & 'Calendar.php' Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[8] SecurityFocus, March 19, 2003.
[9] Corsaire Security Advisory, March 7, 2003.
[10] Bugtraq, March 18, 2003.
[11] Centaura Technologies Security Research Lab Advisory, CTADVILB004, March 7, 2003.
[12] Bugtraq, March 18, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
DeleGate [13, 14]	Windows, Unix	DeleGate 7.9.11	A buffer overflow vulnerability exists in the HTTP Proxy component due to insufficient bounds checking of the 'User-Agent:' field, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.delegate.org/delegate/download/ **OpenPKG:** ftp://ftp.openpkg.org/release/1.1/UPD/delegate-7.9.11-1.1.1.src.rpm	DeleGate 'User-Agent:' Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Epic[15]	Unix	Epic4 1.0.1, 1.1.7 .20020907	A buffer overflow vulnerability exists in 'User_Cmd_Returned' because some types of server replies are not properly handled, which could let a malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.	Epic Userhost_Cmd _Returned Buffer Overflow	Medium	Bug discussed in newsgroups and websites.
Epic[16]	Unix	Epic4 1.0.1, 1.1.7 .20020907	A buffer overflow vulnerability exists in the status bar because server replies are not handled properly, which could let a malicious user obtain unauthorized access.	No workaround or patch available at time of publishing.	Epic Status Bar Buffer Overflow	Medium	Bug discussed in newsgroups and websites.
Epic[17]	Unix	Epic4 1.1.7 .20020907	A vulnerability exists in the 'PRIVMSG' command due to insufficient bounds checking, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary commands.	No workaround or patch available at time of publishing.	EPIC PRIVMSG Remote Heap Corruption	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Ethereal Group[18, 19, 20, 21]	Unix	Ethereal 0.8.18	Two vulnerabilities exist: a format string vulnerability exists in the SOCKS dissector, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code; and a vulnerability exists in the NTLMSSP dissector, which could let a malicious user execute arbitrary code.	Upgrade available at: http://www.ethereal.com/distribution/ethereal-0.9.10.tar.gz **Debian:** http://security.debian.org/pool/updates/main/e/ethereal/	Ethereal SOCKS Dissector Format String & NTLMSSP Overflow CVE Name: CAN-2003-0081	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Exploit scripts have been published.

[13] SecureNet Service (LAC) Advisory, No.63, March 10, 2003.
[14] OpenPKG Security Advisory, OpenPKG-SA-2003.023, March 19, 2003.
[15] SecurityFocus, March 14, 2003.
[16] Bugtraq, March 13, 2003.
[17] Bugtraq, March 13, 2003.
[18] Georgi Guninski Security Advisory #60, March 8, 2003.
[19] Ethereal Advisory, enpa-sa-00008, March 7, 2003.
[20] Debian Security Advisory, DSA 258-1, March 10, 2003.
[21] Gentoo Linux Security Announcement, 200303-10, March 9, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
eZ Systems[22]	Windows, Unix	eZ Publish 2.2.7	Several vulnerabilities exist: a Cross-Site Scripting vulnerability exists due to insufficient sanitization of user-supplied URI parameters, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability exists because malicious HTML and script code that is contained in logging requests is allowed, which could let a malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	eZ Publish Cross-Site Scripting & HTML Injection	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
file[23, 24, 25] ***More updates issued***[26, 27, 28, 29]	**Unix**	**file 3.28, 3.30, 3.32-3.37, 3.39, 3.40**	**A buffer overflow vulnerability exists in the file utility ELF parsing routines, which could let a malicious user cause a Denial of Service and potentially execute arbitrary code.**	**Upgrade available at:** ftp://ftp.gw.com/mirrors/pub/unix/file/file-3.41.tar.gz **RedHat:** **ftp://updates.redhat.com/** **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** **OpenPKG:** **ftp://ftp.openpkg.org/** ***NetBSD:*** **ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2003-003.txt.asc** ***Debian:*** **http://security.debian.org/pool/updates/main/f/file/** ***Trustix:*** **http://www.trustix.net/pub/Trustix/updates/** ***SuSE:*** **ftp://ftp.suse.com/pub/suse**	**File ELF Routine Buffer Overflow** **CVE Name: CAN-2003-0102**	**Low/High** **(High if arbitrary code can be executed)**	**Bug discussed in newsgroups and websites. Exploit script has been published.**
Francisco Burzi[30]	Windows, Unix	PHP-Nuke 5.5, 6.0	A path disclosure vulnerability exists in 'print.php' file, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	PHPNuke 'print.php' File Path Disclosure	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published

[22] Bugtraq, March 18, 2003.
[23] OpenPKG Security Advisory, OpenPKG-SA-2003.017, March 4, 2 003.
[24] Mandrake Linux Security Update Advisory, MDKSA-2003:030, March 6, 2003.
[25] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:086-07, March 7, 2003.
[26] NetBSD Security Advisory, 2003-003, March 12, 2003.
[27] Debian Security Advisory, DSA-260-1, March 13, 2003.
[28] Trustix Secure Linux Bugfix Advisory, TSL-2003-0006, March 18, 2003.
[29] SuSE Security Announcement, SuSE-SA:2003:017, March 21, 2003.
[30] Bugtraq, March 16, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Francisco Burzi[31]	Windows, Unix	PHP-Nuke 6.0	Multiple SQL injection vulnerabilities exist in the Forums scripts and 'Private_Messages' module due to insufficient sanitization of user-supplied data, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Multiple PHP-Nuke Forums/Private_Messages SQL Injection	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Francisco Burzi[32]	Windows, Unix	PHP-Nuke 6.0	Multiple SQL injection vulnerabilities exist in the 'Members_List' and 'Your_Account' modules due to insufficient sanitization of user-supplied data, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	PHP-Nuke Multiple SQL Injection	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
GNOME [33]	Unix	Gnome-lokkit 0.50-21	A vulnerability exists because rules for the FORWARD rule chain are not properly generated, which could leave a machine exposed if packet forwarding is enabled.	**RedHat:** ftp://updates.redhat.com/8.0/en/os/i386/	Gnome-lokkit Forward Chain Rule CVE Name: CAN-2003-0080	Medium	Bug discussed in newsgroups and websites.
GNU[34]	Unix	Transport Layer Security Library 0.5.11	A vulnerability exists because information is leaked through the analysis of the timing of certain operations, which could let a malicious user obtain sensitive information.	Upgrade available at: ftp://gnutls.hellug.gr/pub/gnutls/gnutls-0.8.3.tar.gz	TLS Timing Information Leakage	Medium	Bug discussed in newsgroups and websites.
Gzip.org [35] ***More updates issued*** [36, 37]	**Unix**	**zlib 1.1.4**	**A buffer overflow vulnerability exists in the compression library due to insufficient bounds checking of user-supplied data to the gzprintf() function, which could let a malicious user execute arbitrary instructions.**	**OpenPKG:** http://www.openpkg.org/security/OpenPKG-SA-2003.015-zlib.html ***SCO:*** ftp://ftp.sco.com/pub/updates/OpenLinux ***Mandrake:*** http://www.mandrakesecure.net/en/ftp.php	**Zlib gzprintf() Buffer Overflow** **CVE Name: CAN-2003-0107**	**High**	**Bug discussed in newsgroups and websites. Proof of Concept exploits have been published.**

[31] SecurityFocus, March 10, 2003.
[32] Bugtraq, March 6, 2003.
[33] Red Hat Security Advisory, RHSA-2003:072-00, March 17, 2003.
[34] SecurityFocus, March 5, 2003.
[35] OpenPKG Security Advisory, OpenPKG-SA-2003.015, March 4, 2003.
[36] SCO Security Advisory, CSSA-2003-011.0, March 10, 2003.
[37] Mandrake Linux Security Update Advisory, MDKSA-2003:033, March 18, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Hewlett Packard Company [38]	Unix	Compaq Tru64 4.0g, 4.0g PK3 (BL17), 4.0f, 4.0f PK7 (BL18), PK6 (BL17), 5.0a, 5.0a PK3 (BL17), 5.1a, 5.1a PK3 (BL3), PK2 (BL2), PK1 (BL1), 5.1, 5.1 PK6 (BL20), PK5 (BL19), PK4 (BL18), PK3 (BL17); HP HP-UX 11I, 8.0-8.2, 8.4-8.9, 9.0, 9.1, 9.3-9.10, 10.01, 10.0, 10.1, 10.8-10.10, 10.16, 10.20 SIS, 10.20 Series 700 & 800, 10.20, 10.24, 10.26, 10.30, 10.34, 11.04, 11.0, 11.11, 11.20, 11.22	A vulnerability exists because I/O that are opened by a setuid process may be assigned file descriptors equivalent to those used by the C library as 'standard input', 'standard output', and 'standard error,' which could let an untrusted malicious user write data to sensitive I/O channels and possibly compromise root.	Patches available at: ftp://ftp1.support.compaq.com/public/unix/	HP Tru64/ HP-UX C Library Standard I/O File Descriptor	Medium/ **High** **(High if root can be compro-mised)**	Bug discussed in newsgroups and websites.
Hewlett Packard Company [39]	Unix	HP-UX (VVOS) 11.0 4	A vulnerability exists in the VVOS HFS file system, which could let a malicious user obtain unauthorized access.	Patch available at: http://itrc.hp.com HP Patch PHKL_28401	HP VVOS HFS Unauthorized Access	Medium	Bug discussed in newsgroups and websites.

[38] Hewlett-Packard Company Software Security Response Team Bulletin, SSRT0845U, March 18, 2003.
[39] Hewlett-Packard Company Security Bulletin, HPSBUX0303-247, March 11, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Hewlett Packard Company [40]	Multiple	JetDirect J6038A	Several unspecified vulnerabilities have been reported in J6038A JetDirect 310x Print Servers running version Q.24.06 firmware, which could let a malicious user cause a Denial of Service and obtain unauthorized access.	Upgrades are available via the HP Download Manager at: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=bpj06917 Upgrades are available via Web Jetadmin at: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=bpj06529	HP J6038A JetDirect 310x Print Server For Fast Ethernet Unspecified Vulnerabilities	Low/ Medium (Medium if unauthor-ized access can be obtained)	Bug discussed in newsgroups and websites.
Holger Lamm[41]	Unix	PGP4Pine 1.75.6	A buffer overflow vulnerability exists in the fileVerifyDecryptMenu() function due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	PGP4Pine fileVerify DecryptMenu() Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
IBM Lotus[42]	Windows NT 4.0/2000, Unix	Lotus Domino 4.6.1	A remote Denial of Service vulnerability exists in the NotesRPC authentication protocol.	Upgrade available at: http://www.14software.ibm.com//webapp/download/search.jsp?go=y&rs=ESD-DMNTSRVRi&sb=r	IBM Lotus Notes Remote Denial of Service CVE Name: CAN-2003-0122	Low	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
IBM Lotus[43]	Windows NT 4.0/2000, Unix	Lotus Domino 4.6.1	A buffer overflow vulnerability exists in the Web Retriever program when an overly long HTTP status line message is submitted, which could let a remote malicious user cause a Denial of Service.	Upgrade available at: http://www.14software.ibm.com//webapp/download/search.jsp?go=y&rs=ESD-DMNTSRVRi&sb=r	Lotus Notes/Domino Web Retriever Buffer Overflow Denial of Service CVE Name: CAN-2003-0123	Low	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
IBM Lotus[44]	Windows NT 4.0/2000, Unix	Lotus Domino 4.6.1	A vulnerability exists in the LDAP protocol, which could let a malicious user execute arbitrary code.	Upgrade available at: http://www14.software.ibm.com/webapp/download/search.jsp?go=y&rs=ESD-DMNTSRVRi&sb=r	Lotus Notes/Domino LDAP Service CVE Name: CAN-2001-1311	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

[40] Hewlett-Packard Company Security Bulletin, HPSBMI0303-002, March 12, 2003.
[41] Securiteam, March 16, 2003.
[42] Rapid7, Inc. Security Advisory, R7-0010, March 12, 2003.
[43] Rapid7, Inc. Security Advisory, R7-0011, March 13, 2003.
[44] Rapid7, Inc. Security Advisory, R7-0012, March 12, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Jaco Buddy[45]	Unix	JacoBuddy 3.0 b	Several vulnerabilities exist: a Cross-Site Scripting vulnerability exists in the Chat Module due to insufficient filtering of user-supplied input, which could let a malicious user execute arbitrary script or HTML code; and a vulnerability exists in the 'buddy.php' file, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	JacoBuddy Chat Module Cross-Site Scripting & 'buddy.php' File	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required.
LBL[46] ***More patches releases[47, 48]*** ***SuSE releases patch[49]***	**Unix**	**tcpdump 3.4 a6, 3.4, 3.5, 3.5.2, 3.6.2**	**A vulnerability exists due to a miscalculation in the use of the sizeof operator, which could let a malicious user cause a Denial of Service or execution of arbitrary code.**	**SCO:** **ftp://ftp.sco.com/pub/updates/OpenLinux/** **Trustix:** http://www.trustix.net/pub/Trustix/updates/ ***Debian:*** **http://security.debian.org/pool/updates/main/t/tcpdump/** *Mandrake:* **http://www.mandrakesecure.net/en/ftp.php** ***SuSE:*** **ftp://ftp.suse.com/pub/suse**	**TCPDump Memory Corruption**	**Low/High** **(High if arbitrary code can be executed)**	**Bug discussed in newsgroups and websites.**
LBL[50, 51, 52, 53, 54] ***SuSE releases upgrade[55]***	**Unix**	**tcpdump 3.5.2, 3.6.2, 3.7, 3.7.1**	**A remote Denial of Service vulnerability exists when maliciously formatted ISAKMP packets are submitted.**	**Upgrade available at:** **http://www.tcpdump.org/release/tcpdump-3.7.2.tar.gz** **Debian:** **http://security.debian.org/pool/updates/main/t/tcpdump/** **OpenPKG:** **ftp://ftp.openpkg.org/release/1.2/UPD/tcpdump-3.7.1-1.2.1.src.rpm** **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** ***SuSE:*** **ftp://ftp.suse.com/pub/suse**	**TCPDump Malformed ISAKMP Packet Remote Denial of Service** **CVE Name: CAN-2003-0108**	**Low**	**Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.**

[45] Securiteam, March 9, 2003.
[46] SCO Security Advisory, CSSA-2002-050.0, November 20, 2002.
[47] Debian Security Advisory, DSA 255-1, February 27, 2003.
[48] Mandrake Linux Security Update Advisory, MDKSA-2003:027, March 3, 2003.
[49] SuSE Security Announcement, SuSE-SA:2003:0015, March 13, 2003.
[50] iDEFENSE Security Advisory, February 27, 2003.
[51] Debian Security Advisory, DSA 255-1, February 27, 2003.
[52] Mandrake Linux Security Update Advisory, MDKSA-2003:027, March 3, 2003.
[53] OpenPKG Security Advisory, OpenPKG-SA-2003.014, March 4, 2003.
[54] Gentoo Linux Security Announcement, 200303-5, March 5, 2003.
[55] SuSE Security Announcement, SuSE-SA:2003:0015. March 13, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
LBL[56]	Unix	tcpdump 3.5.2, 3.6.2, 3.7, 3.7.1	A remote Denial of Service vulnerability exists when a malicious user submits a specially crafted RADIUS network packet.	**Debian:** http://security.debian.org/pool/updates/main/t/tcpdump/	TCPDump Malformed RADIUS Packet Remote Denial of Service CVE Name: CAN-2003-0093	Low	Bug discussed in newsgroups and websites.
lxr.sourceforge.net [57]	Unix	Cross Referencer LXR 0.3	A vulnerability exists due to insufficient sanitization of user-supplied input via URI parameters, which could let a remote malicious user obtain sensitive information.	**Debian:** http://security.debian.org/pool/updates/main/l/lxr/lxr_0.3-3_sparc.deb	LXR Cross-Referencer Sensitive Information	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Mambo[58]	Windows, Unix	Mambo Site Server 4.0.10	A Cross-Site Scripting vulnerability exists in the 'index.php' script due to insufficient sanitization of user-supplied URI parameters, which could let a malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	Mambo Site Server 'index.php' Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Matthias Etienne [59]	Windows	PHPPing 0.1	An input validation vulnerability exists in the 'PHP ping' script due to insufficient sanitization of shell metacharacters, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	PHPPing Remote Command Execution	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
McAfee[60]	Windows 2000	ePolicy Orchestrator 2.5.1	A format string vulnerability exists when HTTP GET requests that contain format specifiers are processed, which could let a remote malicious user execute arbitrary commands with SYSTEM privileges.	Contact the vendor to obtain patch: http://www.nai.com/naicommon/aboutnai/contact/intro.asp#software-support	ePolicy Orchestrator HTTP GET Request Format String CVE Name: CAN-2002-0690	**High**	Bug discussed in newsgroups and websites.
McAfee[61]	Windows 2000	ePolicy Orchestrator 2.5.1	A vulnerability exists due to a lack of authentication, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	ePolicy Orchestrator Authentication	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[56] Debian Security Advisory, DSA 261-1, March 14, 2003.
[57] Debian Security Advisory, DSA 264-1, March 19, 2003.
[58] Bugtraq, March 18, 2003.
[59] Security Corporation Security Advisory, SCSA-009, March 6, 2003.
[60] @stake, Inc. Security Advisory, a031703-1, March 17, 2003.
[61] @stake, Inc. Security Advisory, a031703-1, March 17, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [62]	Windows 2000	Internet Explorer 5.5 SP2	A buffer overflow vulnerability exists when malformed '.mht' web archive pages are processed due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Internet Explorer .MHT File Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Microsoft [63]	Windows 2000	ISA Server 2000, 2000 SP1	A remote Denial of Service vulnerability exists in the DNS intrusion detection application filter because specific types of requests when scanning incoming DNS requests are not handled properly.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-009.asp	ISA Server DNS Intrusion Filter Denial of Service CVE Name: CAN-2003-0011	Low	Bug discussed in newsgroups and websites.
Microsoft [64]	Windows 2000	Windows 2000 Advanced Server, SP1-SP3, Datacenter Server, SP1-SP3, Profes-sional, SP1-SP3, 2000 Server, SP1-SP3, Terminal Services, SP1-SP3	A buffer overflow vulnerability exists in the Help facility due to insufficient bounds checking on .cnt files, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Windows 2000 Help Facility .CNT File Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Microsoft [65]	Windows 2000	Windows 2000, ISS 5.0	A buffer overflow vulnerability exists in the Windows component used by Web-based Distributed Authoring and Versioning (WebDAV) due to insufficient bounds checking on data, which could let a remote malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-007.asp	Windows 2000 WebDAV Buffer Overflow CVE Name: CAN-2003-0109	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

[62] Canon System Solutions Inc. Security Alert, March 10, 2003.
[63] Microsoft Security Bulletin, MS03-009, March 19, 2003.
[64] Bugtraq, March 9, 2003.
[65] Microsoft Security Bulletin, MS03-007 V1.1, March 18, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [66]	Windows 98/ME NT 4.0/2000, XP	Windows 2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Profes-sional, SP1-SP3, 2000 Server, SP1-SP3, 2000 Terminal Services, SP1-SP3, Windows 98, SE, ME, Windows NT Enterprise Server 4.0, SP1-SP6a, NT Server 4.0, SP1-SP6a, NT Terminal Server 4.0, SP1-SP6a, NT Work-station 4.0, SP1-SP6a, XP Home, SP1, XP Profes-sional, XP1	A buffer overflow vulnerability exists in the Microsoft Script Engine for JScript (JScript.dll) due to the way information is processed, which could let a remote malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-008.asp	Windows Script Engine JScript.DLL Buffer Overflow CVE Name: CAN-2003-0010	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Microsoft [67]	Windows XP	Windows XP Home SP1	A vulnerability exists when the system is started in Safe Mode, which could let a malicious user obtain unauthorized access. *Note: This vulnerability is only present when the Windows XP "Welcome Screen" is enabled.*	No workaround or patch available at time of publishing.	Windows XP "Welcome Screen"	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[66] Microsoft Security Bulletin, MS03-008 V1.1, March 21, 2003.
[67] Eitan Caspi Security Advisory, EC-SA-01.2003, March 7, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [68]	Windows 2000, XP	Windows 2000 Advanced Server, SP1-SP3, Datacenter Server, SP1-SP3, Profes-sional, SP1-SP3, 2000 Server, SP1-SP3, 2000 Terminal Services, SP1-SP3, XP 64-bit Edition, SP1, XP Home, SP1, XP Profes-sional, SP1	A vulnerability exists in the PostMessage API, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Windows PostMessage API Information Disclosure	Medium	Bug discussed in newsgroups and websites.
MIT[69]	Unix	Kerberos 4 Protocol	Multiple cryptographic vulnerabilities exist: a vulnerability exists in the xdrmem_getbytes() function due to faulty length checks, which could let a malicious user cause a Denial of Service or obtain unauthorized access to sensitive information; a vulnerability exists which could let a malicious user impersonate any principal in a realm that could result in a root-level compromise of the Domain Controller root-level compromise; and a vulnerability exists in the krb4 implementation that allows fabrication of Kerberos 4 tickets for unauthorized client principals if triple-DES keys are used to key Kerberos 4 services.	Patch available for Kerberos 5 with the affected Kerberos 4 code at: http://web.mit.edu/kerberos/www/advisories/2003-004-krb4_patchkit.tar.gz *Note: This patch is not for the Kerberos 4 standalone code.*	Multiple Cryptographic Weaknesses in Kerberos 4	Low/ Medium/ **High** **(Low if a DoS, Medium is sensitive informa-tion can be obtained, and High if a root compro-mise)**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Multiple Vendors[70]	Unix	Debian Linux 3.0 ia-32	A Denial of Service vulnerability exists because some operating systems do not handle specific types of 802.11b traffic properly.	No workaround or patch available at time of publishing.	Multiple Vendor 802.11b Authentication-Failed Denial of Service	Low	Bug discussed in newsgroups and websites.

[68] Bugtraq, March 13, 2003.
[69] MIT krb5 Security Advisory, MITKRB5-SA-2003-003, March 19, 2003.
[70] Bugtraq, March 11, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[71]	Unix	FreeBSD 2.2	A buffer overflow vulnerability exists due to the way some types of requests are handled in lprm, which could let a malicious user execute arbitrary code.	**SuSE:** ftp://ftp.suse.com/pub/suse/	Multiple Vendor LPRM Local Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Multiple Vendors[72]	Windows, Unix	IBM JDK 1.3.1; Sun JRE (Linux, Solaris, Windows Production Release) 1.3.1-1.3.1_07, 1.4-1.4.0_03, 1.4.1, 1.4.1_01, Sun SDK (Linux, Solaris, Windows Production Release) 1.3.1-1.3.1_07, 1.4-1.4.0_03, 1.4.1, 1.4.1_01	A Denial of Service vulnerability exists in several java.util.zip implementations due to insufficient checks to see whether the parameters are NULL values.	Upgrade to Sun JDK 1.4.1_02 available at: http://java.sun.com/j2se/1.4/	Multiple Vendor Java Virtual Machine java.util.zip Null Value Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Multiple Vendors[73, 74, 75, 76]	Unix	Linux kernel 2.2-2.2.24, 2.4-2.4.21 pre1	A vulnerability exists in the ptrace() system call due to a failure to restrict trace permissions on some root spawned processes, which could let a malicious user obtain root access.	Upgrade available at: ftp://ftp.kernel.org/pub/linux/kernel/v2.2/linux-2.2.25.tar.gz **RedHat:** ftp://updates.redhat.com/ **Engarde:** ftp://ftp.engardelinux.org/pub/engarde/stable/updates/ **Trustix:** http://www.trustix.net/pub/Trustix/updates/	Linux Kernel Root Access CVE Name: CAN-2003-0127	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.

[71] SuSE Security Announcement, SuSE-SA:2003:0014, March 13, 2003.
[72] Bugtraq, March 14, 2003.
[73] Red Hat Security Advisory, RHSA-2003:098-00, March 17, 2003.
[74] EnGarde Secure Linux Security Advisory, ESA-20030318-009, March 18, 2003.
[75] Trustix Secure Linux Security Advisory, TSLSA-2003-0007, March 18, 2003.
[76] Red Hat Security Advisory, RHSA-2003:088-01, March 19, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[77, 78]	Unix	Cray UNICOS 6.0, 6.0 E, 6.1, 7.0, 8.0, 8.3, 9.0, 9.0.2.5, 9.2, 9.2.4; FreeBSD 4.0- 4.6, 4.7, 5.0, 4.1.1–4.7 Stable & Release; GNU glibc 2.1-2.1.3, 2.2-2.2.5, 2.3-2.3.2; HP HP-UX 10.20 Series 700 & 800, 10.20, 10.24, 11.04, 11.0, 11.11, 11.20, 11.22; IBM AIX 4.3.3, 5.1, 5.2; MIT Kerberos 5 1.2-1.2.7; OpenAFS 1.0-1.3.2; OpenBSD 2.0-3.2; SGI IRIX 6.5-6.5.20, 6.5m-6.5.20m, 6.5f-6.5.20f; Sun Solaris 2.5.1, 2.5.1_x86, 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86,, 9.0, 9.0_x86	An integer overflow vulnerability exists in the xdrmem_getbytes() function that is distributed as part of the Sun Microsystems XDR library, which could let a remote malicious user execute arbitrary code.	**FreeBSD:** ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-03:05/xdr-4.patch **SCO:** ftp://ftp.sco.com/pub/updates/OpenLinux/ **MIT:** http://web.mit.edu/kerberos/www/advisories/2003-003-xdr_patch.txt **RedHat:** ftp://updates.redhat.com/ **IBM:** http://techsupport.services.ibm.com/r **FreeBSD:** ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-03:05/xdr-4.patch	Sun XDR Library xdrmem_getbytes() Integer Overflow CVE Name: CAN-2003-0028	High	Bug discussed in newsgroups and websites.

[77] eEye Security Advisory, AD20030318, March 19, 2003.
[78] CERT® Advisory, CA-2003-10, March 19, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[79, 80, 81, 82]	Unix	OpenPKG Current, OpenPKG 1.1, 1.2; OpenSSL Project OpenSSL 0.9.6, 0.9.6a-0.9.6I, 0.9.7, 0.9.7a	A side-channel attack in the OpenSSL implementation has been published in a recent paper, which could let a remote malicious user obtain the RSA private key of a target server.	**OpenPKG:** ftp://ftp.openpkg.org/ **Trustix:** ftp://ftp.trustix.net/pub/Trustix/updates/ **Engarde:** ftp://ftp.engardelinux.org/pub/engarde/stable/updates/ **OpenBSD:** ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.1/common/024_blinding.patch	OpenSSL Timing Attack RSA Private Key Information Disclosure CVE Name: CAN-2003-0131	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Multiple Vendors[83, 84, 85, 86, 87, 88, 89, 90]	MacOS X 10.0.4, 10.2x, Unix	HP CIFS/9000 Server A.01.09.01, A.01.09, A.01.08.01, A.01.08, A.01.07, A.01.06, A.01.05; Samba Samba 2.0.0-2.0.10, 2.2.0, 2.2.0a, 2.2.0, 2.2.2-2.2.7	A buffer overflow vulnerability exists in the Samba main smbd code, which could let a remote malicious user execute arbitrary code with root privileges; and a race condition vulnerability exists when writing to reg files, which could let a malicious user obtain elevated privileges.	**Samba;** http://download.samba.org/samba/ftp/ **HP Hotfix:** ftp://samba:samba@hprc.external.hp.com/ **SuSE:** ftp://ftp.suse.com/pub/suse/ **OpenPKG:** ftp://ftp.openpkg.org/release **Mandrake:** http://www.mandrakesecure.net/en/ftp.php **RedHat:** ftp://updates.redhat.com/ **SGI:** http://freeware.sgi.com/beta/fw_samba-2.2.8.tardist **Debian:** http://security.debian.org/pool/updates/main/s/samba/ **Trustix:** http://www.trustix.net/pub/Trustix/updates/	Samba SMB/CIFS Buffer Overflow & Reg File Race Condition CVE Names: CAN-2003-0085, CAN-2003-0086	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required for the race condition vulnerability. Vulnerability has appeared in the press and other public media.

[79] OpenPKG Security Advisory, OpenPKG-SA-2003.019, March 18, 2003.
[80] OpenPKG Security Advisory, OpenPKG-SA-2003.020, March 18, 2003.
[81] Trustix Secure Linux Security Advisory, TSLSA-2003-0010, March 18, 2003.
[82] EnGarde Secure Linux Security Advisory, ESA-20030320-010, March 20, 2003.
[83] Debian Security Advisory, DSA-262-1, March 15, 2003.
[84] Mandrake Linux Security Update Advisory, MDKSA-2003:032, March 15, 2003.
[85] Red Hat Security Advisory, RHSA-2003:095-01, March 17, 2003.
[86] Hewlett-Packard Company Security Bulletin, HPSBUX0303-251, March 18, 2003.
[87] OpenPKG Security Advisory, OpenPKG-SA-2003.021, March 18 2003.
[88] Trustix Secure Linux Security Advisory, TSLSA-2003-0011, March 18, 2003.
[89] SGI Security Advisory, 20030302-01-I, March 19, 2003.
[90] SuSE Security Announcement, SuSE-SA:2003:015, March 19, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multi-Tech Systems[91]	Multiple	Route Finder 550 VPN	Several vulnerabilities exist: a vulnerability exists in HTTP GET requests due to insufficient bounds checking, which could let a remote malicious user cause a Denial of Service and execute arbitrary code; and a vulnerability exists in the default configuration because a default username and blank password exists, which could let a remote malicious user obtain administrative access.	Upgrade available at: http://www.multitech.com/SUPPORT/SOHO_VPN/firmware.asp	Multitech RouteFinder Remote Memory Corruption	Low/**High** **(Low if a Denial of Service, and High if arbitrary code can be executed or adminis-trative access can be obtained)**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Mutt[92, 93]	Unix	Mutt 1.3.16, 1.3.17, 1.3.22, 1.3.24, 1.3.25, 1.4.0, 1.5.3	A buffer overflow vulnerability exists because remote internationalized folders are not properly handled, which could let a malicious user execute arbitrary code.	Upgrade available at: ftp://ftp.mutt.org/mutt/mutt-1.4.1i.tar.gz **OpenPKG:** ftp://ftp.openpkg.org/release	Mutt Remote Folder Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
MyABra CaDaWeb Develop-ment Team[94]	Unix	MyABra CaDaWeb 1.0	Several vulnerabilities exist: a path disclosure vulnerability exists in error messages when invalid requests are handled, which could let a remote malicious user obtain sensitive information; and a Cross-Site Scripting vulnerability exists in the search engine, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	MyAbraCada Web Path Disclosure & Cross-Site Scripting	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Path disclosure vulnerability can be exploited via a web browser. There is no exploit code required. for the Cross-Site Scripting vulnerability.
MySQL[95]	Unix	AB Control Center 0.8.8	A vulnerability exists because configuration and connection files are installed world-readable, which could let a malicious user obtain sensitive information.	Upgrade available at: http://www.mysql.com/downloads/mysqlcc.html	MySQL Control Center Insecure Default File Permission	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
MySQL AB[96, 97, 98]	Unix	MySQL 3.23.52	A vulnerability exists in the 'mysqld' service, which could let a malicious user obtain elevated privileges as root.	Upgrade available at: http://www.mysql.com/downloads/mysql-3.23.html **OpenPKG:** ftp.openpkg.org **Trustix:** http://www.trustix.net/pub/Trustix/updates/	MySQL 'mysqld' Elevated Privileges	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[91] SecurityTracker Alert ID, 1006267, March 11, 2003.
[92] Core Security Technologies Advisory, CORE-20030304-02, March 20, 2003.
[93] OpenPKG Security Advisory, OpenPKG-SA-2003.025, March 20, 2003.
[94] Security Corporation Security Advisory, SCSA-010, March 17, 2003.
[95] Gentoo Linux Security Announcement, 200303-7, March 7, 2003.
[96] OpenPKG Security Advisory, OpenPKG-SA-2003.022, March 18, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Nara Vision[99]	Unix	Kebi Academy 2001	A Directory Traversal vulnerability exists due to insufficient sanitization of input supplied via URI parameters, which could let a remote malicious user obtain sensitive information or execute arbitrary code.	No workaround or patch available at time of publishing.	Kebi Academy 2001 Input Validation	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
NetScreen [100]	Multiple	ScreenOS 4.0 -DIAL	A vulnerability exists because under certain conditions devices may lose their configurations and revert to factory default settings, which could let a remote malicious user cause a Denial of Service.	Update available at: http://www.netscreen.com/support/updates.asp	ScreenOS Configuration Loss	Low	Bug discussed in newsgroups and websites.
Network Associates [101]	Multiple	PGP 7.1	A vulnerability exists due to the way PGP handles signature verification, which could let a malicious user execute arbitrary OLE objects.	No workaround or patch available at time of publishing.	PGP Embedded OLE Object Verification	**High**	Bug discussed in newsgroups and websites.
Noah Grey[102]	Multiple	Greymatter 1.1 b	A vulnerability exists in the weblog due to improper sanitization of untrusted input, which could let an unauthorized remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	GreyMatter WebLog Untrusted Input	**High**	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Nokia[103]	Multiple	DX200 (SGSN)	A vulnerability exists in the Simple Network Management Protocol (SNMP) daemon because remote requests for information are not handled properly, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	SGSN DX200 Remote SNMP Information Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability may be exploited with an SNMP client.
Novell[104]	Unix	FTPSERV. NLM 10.19	A Denial of Service vulnerability because some types of input are not handled properly due to FTP protocol implementations.	Patch available at: http://support.novell.com/servlet/filedownload/ftf/ftpservl.exe	NetWare FTPServ Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
onedotoh [105]	Windows, Unix	sFile Manager 0.17	A vulnerability exists in the 'fm.php' script due to insufficient filtering of HTML tags from file names, which could let a remote malicious user execute arbitrary HTML code.	Upgrade available at: http://freshmeat.net/releases/115223/	Simple File Manager 'fm.php' Script	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.

[97] Gentoo Linux Security Announcement, 200303-14, March 18, 2003.
[98] Trustix Secure Linux Security Advisory, 2003-0009, March 18, 2003.
[99] INetCop Security Advisory, 2002-0x82-013, March 17, 2003.
[100] NetScreen Security Alert, 56305, March 6, 2003.
[101] Bugtraq, March 12, 2003.
[102] SecurityFocus, March 10, 2003.
[103] Securiteam, March 16, 2003.
[104] Technical Information Document, TID2965109, March 7, 2003.
[105] SecurityFocus, March 6, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Opera Software [106]	Windows	Opera Web Browser 6.0.5 win32	A buffer overflow vulnerability exists due to insufficient bounds checking when copying file names to a temporary buffer, which could let a malicious user execute arbitrary commands.	Upgrade available at: http://www.opera.com/download/	Opera Long Filename Download Buffer Overrun	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published. Vulnerability has appeared in the press and other public media.
Outblaze [107]	Multiple	Webmail	A vulnerability exists because cookie-based authentication mechanisms can be bypassed, which could let a malicious user obtain sensitive information and full access to the victims e-mail account.	No workaround or patch available at time of publishing.	Webmail Authentication Bypass	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
People Soft[108]	Windows NT 4.0/2000, Unix	People Tools 8.10	A vulnerability exists in the 'SchedulerTransfer' Java servlet due to insufficient validation of user-supplied data, which could let a remote malicious user execute arbitrary commands.	Users should contact the vendor for details on obtaining fixes.	PeopleTools Scheduler Transfer Remote Command Execution CVE Name: CAN-2003-0104	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Postgre SQL[109]	Unix	Postgre SQL 7.2	A remote Denial of Service vulnerability exists when authenticating certain users.	No workaround or patch available at time of publishing.	PostgreSQL Remote Denial of Service	Low	Bug discussed in newsgroups and websites.
PostNuke Develop-ment Team[110]	Windows, Unix	PostNuke Phoenix 0.722	Multiple vulnerabilities exist: a vulnerability exists in the 'Members_List' module due to insufficient sanitization of user-supplied input, which could let a malicious user execute arbitrary code; and a Directory Traversal vulnerability exists in the theme handling engine, which could let a remote malicious user obtain sensitive information.	Patch available at: http://download.hostnuke.com	PostNuke Phoenix SQL Injection & Directory Traversal	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required.

[106] Bugtraq, March 11, 2003.
[107] INetCop Security Advisory, 2003-0x82-014.c, March 19, 2003.
[108] Internet Security Systems Security Brief, March 10, 2003.
[109] Mordred Labs advisory 0x0007, March 12, 2003.
[110] Bugtraq, March 9, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Protegrity [111]	Windows 2000	Secure. Data 2.2.3.7, 2.2.3.8	Several vulnerabilities exist: a buffer overflow vulnerability exists in the 'xp_pty_checkusers' function due to insufficient checks, which could let a malicious user obtain elevated privileges; a buffer overflow vulnerability exists in the 'xp_pty_insert' function due to insufficient checks, which could let a malicious user obtain elevated privileges; and a buffer overflow vulnerability exists in the 'xp_pty_select' function due to insufficient checks, which could let a malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.	Secure.Data Multiple Buffer Overflows	Medium	Bug discussed in newsgroups and websites.
Qual-comm[112]	Windows 95/98/ME/ NT 4.0/2000, MacOS 8.1 or later	Eudora 5.0.2	A remote Denial of Service vulnerability exists when a malicious user submits a message that contains a malformed attachment.	Upgrade available at: http://www.eudora.com/email/upgrade/index.html	Eudora Attachment Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Qual-comm[113]	Unix	qpopper 3.1, 4.0.4	An information disclosure vulnerability exists when authenticating, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Qpopper Authentication Information Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Qual-comm[114]	Unix	qpopper 4.0.1	A vulnerability exists when the 'mdef' command is called and a malicious macro name is supplied, which could let a remote malicious user execute arbitrary code.	Upgrade available at: ftp://ftp.qualcomm.com/eudora/servers/unix/popper/beta	Qpopper Remote Memory Corruption	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.

[111] Bugtraq, March 13, 2003.
[112] Securiteam, March 5, 2003.
[113] Bugtraq, March 15, 2003.
[114] Bugtraq, March 10, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
rcII Project[115]	Unix	ircII 20021103, 20020912, 20020403	Several vulnerabilities exist: a buffer overflow vulnerability exists because some functions do not properly account for control characters when attempting to refresh the status bar, which could let a malicious user cause a Denial of Service; a buffer overflow vulnerability exists due to insufficient bounds checking of server-supplied private messages data, which could let a malicious user cause a Denial of Service and possibly execute arbitrary code; and a buffer overflow vulnerability exists in the cannot_join_channel() function due to insufficient bounds checking of server-supplied data, which could let a malicious user cause a Denial of Service and possibly execute arbitrary code.	Upgrade available at: ftp://ircii.warped.com/pub/ircII/ **OpenPKG:** ftp://ftp.openpkg.org/release	ircII Multiple Vulnerabilities	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
RedHat[116]	Unix	PXE Server 2.0 Beta 1	A buffer overflow vulnerability exists when excessive data is submitted to the service, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	PXE Server Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
RSA Security [117]	Windows NT 4.0/2000, Unix	ClearTrust Server 4.7.1 ClearTrust Server 4.6.1.1	Cross-Site Scripting vulnerabilities exist in the login page due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	ClearTrust Login Page Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploits have been published.
SalD Ltd.[118]	Windows 95/98/ME NT 4.0/2000, XP, OS/2, Unix	Dr.Web 4.15	A buffer overflow vulnerability exists in the scanner due to insufficient bounds checking when processing folder names, which could let a malicious user execute arbitrary code with root privileges.	Upgrade available at: http://www.sald.com/	Dr.Web Virus Scanner Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
SaveMy Modem[119]	Windows, Unix	SaveMy Modem 0.11	A buffer overflow vulnerability exists in the 'statusbar_set_text' function, which could let a malicious user execute arbitrary code.	Upgrade available at: http://sourceforge.net/project/showfiles.php?group_id=60848&release_id=145186	SaveMy Modem Statusbar_Set_ Text Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

[115] OpenPKG Security Advisory, OpenPKG-SA-2003.024, March 19, 2003.
[116] Securiteam, March 17, 2003.
[117] Mordred Security Labs Advisory, March 14, 2003.
[118] Securiteam, March 5, 2003.
[119] SecurityFocus, March 11, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
SCO[120]	Unix	Open UNIX 8.0	A vulnerability exists in the /dev/X directory because files are world readable and writable, which could let a malicious user cause a Denial of Service or obtain elevated privileges.	Patch available at: ftp://ftp.sco.com/pub/updates/UnixWare/CSSA-2003-SCO.4.2/basex711.pkg.Z	OpenUnix X Server World Writeable Permissions	Low/ Medium (Medium if elevated privileges can be obtained)	Bug discussed in newsgroups and websites. There is no exploit code required.
Simple Media[121]	Windows, Unix	SimpleBBS 1.0.6	A vulnerability exists because sensitive files are created with world-readable permissions, which could let a remote malicious user obtain sensitive information.	Upgrade available at: http://www.simplemedia.org/sbbs-107-src.zip	SimpleBBS Users.php Insecure File Permissions	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
SIPS[122]	Unix	SIPS 0.2.2	A vulnerability exists due to a lack of authentication when viewing user account information, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	SIPS User Account Authentication	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
SMC[123]	Multiple	Broadband Router SMC7004 VWBR	A vulnerability exists because router administration credentials are stored in a backup archive using plaintext format, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	SMC Router Backup Tool Plaintext Password	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Sun Micro-systems, Inc.[124]	Windows NT 4.0/2000	ONE Application Server 6.0, 6.5	A buffer overflow vulnerability exists in the Connector Module, a Netscape Server Application Programming Interface (NSAPI) plug-in, which could let a remote malicious user execute arbitrary code.	Service Pack available at: http://wwws.sun.com/software/download/products/3e3afb89.html	ONE Application Server Connector NSAPI Module Remote Buffer Overflow CVE Name: CAN-2002-0387	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Sun Micro-systems, Inc.[125]	Unix	Solaris 7.0_x86	A vulnerability exists due to a security issue with how sendmail(1M) handles some $HOME/.forward constructs, which could let an unauthorized malicious user cause a Denial of Service or possibly obtain unauthorized root access.	Patch available at: http://sunsolve.sun.com/pub-cgi/findPatch.pl?patchId=107685&rev=06 Sun Patch 107685-06	Sun Sendmail ".forward" Constructs	Low/**High** **(High if root access can be obtained)**	Bug discussed in newsgroups and websites.

[120] SCO Security Advisory, CSSA-2003-SCO.4.1, March 10, 2003.
[121] SecurityTracker Alert ID, 1006251, March 8, 2003.
[122] Bugtraq, March 18, 2003.
[123] SecurityFocus, March 10, 2003.
[124] @stake, Inc. Security Advisory, A031303-1, March 13, 2003.
[125] Sun(sm) Alert Notification, 50904, March 5, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Sun Micro-systems, Inc.[126] ***Sun updates bulletin***[127] ***Sun releases patches***[128]	**Unix**	**Solaris 2.6, 7, 8, 9**	**A remote Denial of Service vulnerability exists in the 'in.ftpd' daemon.** ***Temporary patches available and updated relief/workaround section.***	**Workaround:** **http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F50240**	**Solaris Remote Denial of Service**	**Low**	**Bug discussed in newsgroups and websites.**
Sun Micro-systems, Inc.[129]	Unix	Solaris 9.0	A Denial of Service vulnerability exits in the UFS file system. *Note: This only occur on UFS file systems that are mounted with the "logging" option enabled.*	Patch available at: http://sunsolve.sun.com Sun Patch 113454-04	Solaris UFS File System Denial of Service	Low	Bug discussed in newsgroups and websites.
Sun Micro-systems, Inc.[130]	Unix	SUN Wlldap 11.8	A buffer overflow vulnerability exists in the SUNWlldap library when an application linked to the LDAP library is used to resolve hostnames of excessive length, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Sun SUNWlldap Library Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Sux Services [131]	Unix	Sux Services 0.2	A vulnerability exists in the implementation of printf() related functions because data supplied by IRC clients is insufficiently sanitized before included in queries to the database, which could let a malicious user obtain sensitive information or corrupt the database.	Upgrade available at: http://prdownloads.sourceforge.net/suxserv/suxserv-0.2.5.tar.gz?download	Sux Services SQL Injection	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Thunder stone Software [132]	Windows NT 4.0	Texis 3.0	An information disclosure vulnerability exists because command line switches as URI parameters may be passed to TEXIS.EXE, which could let a malicious user obtain sensitive information.	Thunderstone has created a fix to resolve the issue. Customers who wish to take advantage of the change are advised to contact Thunderstone technical support.	TEXIS Texis.EXE Information Disclosure	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[126] Sun(sm) Alert, 50240, January 27, 2003.
[127] Sun(sm) Alert, 50240, February 6, 2003.
[128] Sun(sm) Alert, 50240, March 14, 2003
[129] Sun(sm) Alert Notification, 51300, March 11, 2003.
[130] Securiteam, March 16, 2003.
[131] SecurityFocus, March 6, 2003.
[132] Mordred Security Labs Advisory, March 14, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Tower Toppler[133]	Unix	Tower Toppler 0.99.1	A buffer overflow vulnerability exists when a specially crafted argument is supplied to the toppler binary, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Tower Toppler Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Upload Lite[134]	Windows	Upload Lite 3.22	A vulnerability exists because a file can be uploaded two times in a single HTTP POST submission with the same file name for both files, which could let a remote malicious user execute arbitrary CGI code.	No workaround or patch available at time of publishing.	Upload Lite Arbitrary File Upload	High	Bug discussed in newsgroups and websites. There is no exploit code required.
VPOP Mail[135]	Unix	VPOPMail 0.9	A vulnerability exists in the 'vpopmail.php' script due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	VPOPMail 'vpopmail.php' Remote Command Execution	High	Bug discussed in newsgroups and websites. Proof of Concept exploits have been published.
Webdev[136] ***Upgrade now available***[137]	**Windows, Unix**	**Webchat 0.77**	**A vulnerability exists in the 'defines.php' script due to insufficient sanitization of user-supplied data, which could let a remote malicious user execute arbitrary commands.**	***Upgrade available at:*** **http://www.webdev.ro/products/webchat/download.php**	**Webchat Defines.PHP Remote File Include**	High	**Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.**
Wordit Limited 2000[138]	Windows, Unix	Logbook 098b3	An input validation vulnerability exists in the 'logbook.pl' script due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	Logbook Logbook.pl Remote Command Execution	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[133] SecurityTracker Alert ID, 1006191, March 2, 2003.
[134] Securiteam, March 10, 2003.
[135] Bugtraq, March 12, 2003.
[136] Bugtraq, March 3, 2003.
[137] SecurityFocus, March 14, 2003.
[138] Bugtraq, March 7, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Ximian[139, 140]	Unix	Evolution 1.0.3-1.0.8, 1.1.1, 1.2-1.2.2	Multiple vulnerabilities exist: a vulnerability exists in the parsing component, which could let a remote malicious user cause a Denial of Service; a vulnerability exists in the Mail User Agent (MUA) when a maliciously encoded e-mail message is decoded, which could let a remote malicious user cause a Denial of Service; and a vulnerability exists in the Content-ID header, which could let a remote malicious user execute arbitrary code.	**RedHat:** ftp://updates.redhat.com/	Ximian Multiple Vulnerabilities CVE Names: CAN-2003-0128, CAN-2003-0129, CAN-2003-0130	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Exploits has been published.

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between March 7 and March 18, 2003, listed by date of script, script names, script description, and comments. Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing. During this period, 28 scripts, programs, and net-news messages containing holes or exploits were identified. *Note: At times, scripts/techniques may contain names or content that may be considered offensive.*

Date of Script (Reverse Chronological Order)	Script Name	Script Description
March 18, 2003	Finder.pl	Perl script that remotely checks IIS Servers for most of the methods used by WebDAV.
March 17, 2003	Km3.c	Script that exploits the Linux Kernel Root Access vulnerability.

[139] Core Security Technologies Advisory, CORE-2003-03-04-01, March 19, 2003.
[140] Red Hat Security Advisory, RHSA-2003:108-01, March 21, 2003.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
March 17, 2003	Ptrace-kmod.c	Script that exploits the Linux Kernel Root Access vulnerability.
March 16, 2003	**85pxe.c**	**Script that exploits the PXE Server Remote Buffer Overflow vulnerability.**
March 16, 2003	Elfrape2.c	Proof of concept exploit for the File ELF Routine Buffer Overflow vulnerability.
March 15, 2003	**Poptest.cpp**	**Exploit for the Qpopper Authentication Information Disclosure vulnerability.**
March 14, 2003	**Hoagie_solarisldap.c**	**Script that exploits the Sun SUNWlldap Library Buffer Overflow vulnerability.**
March 14, 2003	Openfuck.c	Remote exploit for Apache + OpenSSL v0.9.6d and below vulnerability.
March 14, 2003	Ssl-timing.pdf	A paper written on timing attacks against OpenSSL 0.9.7 that demonstrates how to remotely extract private keys from an OpenSSL-based webserver.
March 13, 2003	Lprmexp.c	Script that exploits the LPRM Local Buffer Overflow vulnerability.
March 12, 2003	**Mailex-gen.c**	**Script that exploits the PGP4Pine Buffer Overflow vulnerability.**
March 12, 2003	Tcpip_lib4.zip	A library for Windows 2000 that allows constructing custom packets, IP spoofing, attacks, and more.
March 12, 2003	USG-ipp.c	IS 5.0 / Windows 2000 mass scanner / rooter.
March 11, 2003	Opera02-dlfnbof_sample.tgz	Exploit for the Opera Long Filename Download Buffer Overrun vulnerability.
March 10, 2003	Ah1.zip	aH scans for open NetBIOS shares on a system and reports them to the user in an easy to use copy and paste format utilizing the net command.
March 10, 2003	**Cpanel.exe**	**Script that exploits the CPanel 5 'gueltbook.cgi' vulnerability.**
March 10, 2003	**Cpanel.pl**	**Perl script that exploits the CPanel 5 'gueltbook.cgi' vulnerability..**
March 10, 2003	**DSR-toppler.pl**	**Perl script that exploits the Tower Toppler Buffer Overflow vulnerability.**
March 10, 2003	**DSR-unreal.c**	**Local exploit for Unreal IRC daemon 3.2 vulnerability.**
March 10, 2003	Elfrape.c	Proof of concept exploit for the File ELF Routine Buffer Overflow vulnerability.
March 10, 2003	Ethereal-0.9.11.tar.gz	a GTK+-based network protocol analyzer, or sniffer, that lets you capture and interactively browse the contents of network frames.
March 10, 2003	Jempiscodes-0.4r1.tgz	Polymorphic Shellcode Generator is a tool that is written in Spanish to mask the final function of shellcode in exploits.
March 10, 2003	Qex.c	Script that exploits the Qpopper Remote Memory Corruption vulnerability.
March 10, 2003	**S0h_Win32hlp.c**	**Script that exploits the Windows 2000 Help Facility .CNT File Buffer Overflow vulnerability.**
March 8, 2003	Raw3sv.pl	Perl script that exploits the Ethereal SOCKS Dissector Format String & NTLMSSP Code Heap Overflow vulnerability.
March 8, 2003	Sockcl.pl	Perl script that exploits the Ethereal SOCKS Dissector Format String & NTLMSSP Code Heap Overflow vulnerability.
March 7, 2003	Bin.exe.zip	Exploit for the MailSweeper Attachment Filter Bypass vulnerability.
March 6, 2003	85deadelf.c	Script that exploits the File ELF Routine Buffer Overflow vulnerability.

Trends

- Over the past few weeks, their have been an increased number of reports of intruder activity involving the exploitation of Null (i.e., non-existent) or weak Administrator passwords on Server Message Block (SMB) file shares used on systems running Windows 2000 or Windows XP. This activity has resulted in the successful compromise of thousands of systems, with home broadband users' systems being a prime target. Recent examples of such activity are the attack tools known as W32/Deloder, GT-bot, sdbot, and W32/Slackor. For more information, see CERT® Advisory CA-2003-08, located at: http://www.cert.org/advisories/CA-2003-08.html.
- **The Department of Homeland Security (DHS), National Infrastructure Protection Center (NIPC) has issued an advisory to heighten awareness of the recently discovered Remote SendMail Header Processing Vulnerability (CAN-2002-1337). NIPC has been working closely with the industry on vulnerability awareness and information dissemination. For more information, see 'Bugs, Holes & Patches' table and DHS/NIPC Advisory 03-004 located at: http://www.nipc.gov/warnings/advisories/2003/03-004.htm.** ***Note: SendMail is the most commonly used Mail Transfer Agent and processes an estimated 50 to 75 percent of all Internet e-mail traffic. System administrators should be aware that many SendMail servers are not typically shielded by perimeter defense applications.*** **Remote malicious users may gain access to other systems through a compromised SendMail server, depending on local configurations.**
- Systems are being compromised through the exploitation of null or weak default 'sa' passwords in Microsoft SQL Server and Microsoft Data Engine.
- Propagation of SQL 'Slammer' or 'Sapphire' malicious code is still causing varied levels of network degradation across the Internet and the compromise of vulnerable machines.
- NIPC has issued an advisory regarding the propagation of an SQL worm. The self-propagating malicious code exploits multiple vulnerabilities in the Resolution Service of Microsoft SQL Server 2000. This worm activity appears to have caused various levels of network degradation across the Internet. In addition to the compromise of vulnerable machines; the apparent effects of this fast-spreading, virus-like infection has overwhelmed the world's digital pipelines and interfered with Web browsing and delivery of e-mail. For more information, see Virus Section, WORM_SQLP1434.A description and NIPC Advisory 03-001.1, located at: http://www.nipc.gov/warnings/advisories/2003/03-001.1updates.htm. For patch information, see:
  - http://www.microsoft.com/security/slammer.asp
  - http://www.microsoft.com/technet/security/bulletin/MS02-061.asp
  - http://www.microsoft.com/technet/security/bulletin/MS02-039.asp
- The CERT/CC has released an advisory regarding a buffer overflow vulnerability in the Microsoft Windows Shell. For more information, see Bugs, Holes & Patches table entry, "Windows XP WMA/MP3 Buffer Overflow" and CERT® Advisory CA-2002-37, located at: http://www.cert.org/advisories/CA-2002-37.html.
- The CERT/CC has released an advisory regarding multiple vendors' implementations of the secure shell (SSH) transport layer protocol contain vulnerabilities that could allow a remote malicious user to execute arbitrary code with the privileges of the SSH process or cause a denial of service. The vulnerabilities affect SSH clients and servers, and they occur before user authentication takes place. For more information, see Bugs, Holes & Patches table entry "Multiple Vendor SSH2 Implementation" and CERT® Advisory CA-2002-36, located at: http://www.cert.org/advisories/CA-2002-36.html.
- The CERT/CC has received reports of increased scanning for NetBIOS services. Probes to port 137/udp may be indicative of such activity.

Viruses

The following virus descriptions encompass new viruses and variations of previously encountered viruses that have been discovered in the last two weeks. The viruses are listed alphabetically by their common name. While these viruses might not all be in wide circulation, it is highly recommended that users update anti-virus programs as often as updates become available. *NOTE: At times, viruses may contain names or content that may be considered offensive.*

CODERED.F (Aliases: W32/CodeRed.f.worm, CodeRed.F, Win32.CodeRed.F, CodeRed.v3, CodeRed.C, CodeRed III, W32.Bady.C, W32/CodeRed.a.worm) (Win32 Worm): This worm is similar to the other variants of CodeRed and makes use of a remote-buffer overflow vulnerability in Microsoft's Internet Information Server (IIS) that can give system level privileges to a malicious user. It drops a backdoor program on an infected Web server, giving a malicious user full access to this Web server, thereby compromising network security. The only difference between this variant and CODERED.C is the trigger date when it restarts the system. The .C variant restarts the system if the year is greater than 2002. This .F variant executes the same routine if the year is greater than or equal to 34952.

IRC.Vale.Worm (Alias: IRC-Worm.generic.bat) (IRC Worm): This is both an IRC worm and a mass mailer. It sends itself to other users using the IRC channel and e-mail. IRC.Vale.Worm is a batch file that includes VBScript code. When IRC.Vale.Worm is executed, it creates a VBScript file that displays messages.

PE_DER.A (Alias: W32.HLLW.DER@mm) (File Infector Virus): This memory-resident and destructive malware overwrites its codes to its target files with the following extensions: jpg, bmp, wav, and exe. It arrives in an e-mail with details as follows:

- Subject: <Computer name>. WORLD TRADE CENTER PICTURES
- Attachment: <Worm copy>

Upon execution, it displays a message box and an OK button, and then displays another message, which differs in each infection. It executes its mass-mailing routine after displaying the messages. After its mass-mailing routine, target files are overwritten. This malware runs on all Windows platforms, Windows 95, 98, ME, NT, 2000, and XP. After mass mailing, it will execute its destructive payload, which is to overwrite files.

PE_SAHAY.B (Aliases: W32/Sahay.worm.b, W32.Sahay.A@mm, I-Worm.Sahay.b, Win32/Sahay.B@mm, Win32/Sahay.B.Worm, Win32.Sahay.B) (File Infector Worm): This variant of PE_SAHAY.A is both a file infector and a worm. To infect files, it attaches a copy of itself at the start of each target, .EXE file, located in the C:\Program Files\mIRC\download folder. To propagate, this malware uses a Visual Basic script component, detected as VBS_SAHAY.B, to send itself to all e-mail addresses listed in the Outlook Address Book. Aside from infecting .EXE files and mass mailing copies of itself, this malware also attempts to clean systems of WORM_YAHA.K and its variants. This PE infecting worm is written in Visual C++ and runs on Windows 95, 98, ME, NT, 2000, and XP.

VBS_GROUCH.A (Aliases: VBS/Cian.A@mm, VBS/Kitro.D.Worm, I-Worm.Cian, VBS.Cian.B worm, VBS.Grouch@mm) (Visual Basic Script Worm): This Visual Basic script worm propagates via Internet Relay Chat, popular peer-to-peer file sharing networks, and e-mail. It infects the Word global template so that it executes every time a document is opened or closed in Microsoft Word. To propagate via e-mail, it sends a copy of itself to addresses found in the Microsoft Outlook address book. This worm, which runs on Windows 95, 98, ME, NT, 2000, and XP, attempts to execute an ineffective payload on May 9 on systems running Windows XP. It tries but fails to delete all files and folders from the current drive.

VBS_PRUNE.A (Aliases: VBS/Carnival.gen@MM, , I-Worm.Prune, VBS/Entice, VBS/FindPeach.A.Worm) (Visual Basic Script Worm): This worm spreads by mass-mailing copies of itself to all recipients listed in the Microsoft Outlook address book. It also spreads across the network and attempts to propagate via Internet Relay Chat (IRC). Buggy codes, however, prevent it from completing its propagation routine via IRC. It sends itself as an attachment in an e-mail with this format:

- Subject: "US Government Material - Iraq Crisis"
- Message Body:<blank>
- Attachment:C:\WINDOWS\UN_Interview.txt.vbs

The viral code indicates that this worm has destructive capabilities of deleting files when the system date is 1-5 of any month. However, it lacks the necessary codes to complete this routine. It runs on Windows 95, 98, NT, 2000, ME, and XP.

VBS.Suconelo (Visual Basic Script Worm): This is an intended mass-mailing worm. The purpose of VBS.Suconelo is to:

- Send itself to the e-mail addresses in the Microsoft Outlook address book
- Delete the files
- Modify the configuration settings
- Display various messages

VBS.Ztin (Visual Basic Script Virus): This is a VBS script that attempts to spread using various peer-to-peer programs. VBS.Ztin may also overwrite .jpg and .jpeg files. The payload of this VBS script includes pinging certain URLs with large packets.

W32.Alco.AB@mm (Win32 Worm): This is a mass-mailing worm that sends itself to all the e-mail addresses that it finds in the .htm and .html files. The e-mail has the following characteristics:

- From: Chief Skaler <admin@evol.com>
- Subject: Evol Worm
- Attachment: Errorlog.exe

The worm copies itself to the default shared folders of the KaZaA, Bearshare, and eDonkey2000 file-sharing networks. The worm also attempts to spread through IRC. This threat is written in the Microsoft Visual Basic programming language.

W32/Deborm-R (Aliases: MultiDropper-FL, Worm.Win32.Deborm.r, Win32/Nebiwo.B, W32.HLLW.Nebiwo) (Win32 Worm): This is a network worm which carries and installs Trojans. When run, the worm searches for shares named C or C$ on the local IP subnet that have no password. If a share is found, the worm will attempt to copy itself to one of the following folders:

- Windows\Start Menu\Programs\Startup
- Documents and Settings\All Users\Start Menu\Programs\Startup
- Winnt\Profiles\All Users\Start Menu\Programs\Startup

W32/Deborm-R will attempt to install the Trojans Troj/Litmus-203, Troj/Sdbot-Fam, and Troj/KillAV-Q. The worm also adds the following registry entry, containing the name of the worm file so that it is run each time Windows is started:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\NAV Live Update

W32/Deloder-A (Aliases: W32.HLLW.Deloder, WORM_DELODER.A) (Win32 Worm): This worm has been reported in the wild. It is a network worm that spreads to random IP addresses and installs a backdoor Trojan. When first run, the worm drops the files Psexec.exe and inst.exe to the current folder and creates the following registry entry so that the worm executable is run automatically each time Windows is started:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\messenger = <pathname of worm>

The worm attempts to connect to port 445 of target computers which is the NetBIOS port for Windows 2000 and XP. W32/Deloder-A copies itself to shares on the remote computer as Dvldr32.exe and tries to install a backdoor Trojan component inst.exe to the startup folders:

- C$\WINNT\All Users\Start Menu\Programs\Startup\,
- C\WINDOWS\Start Menu\Programs\Startup\
- C$\Documents and Settings\All Users\Start Menu\Programs\Startup\inst.exe

so that inst.exe is run automatically each time the target computer is restarted. It queries the remote computer for a valid username and then attempts to logon using a brute force method to crack the password. This involves trying a list of common 'weak' passwords. If the worm is unable to get a valid username, it attempts to logon via the IPC$ share. The worm uses the valid utility Psexec.exe to remotely set the attributes for inst.exe and Dvldr32.exe to read-only, to launch inst.exe and Dvldr32.exe and to disable the network shares C$, D$, E$, F$, IPC$ and ADMIN$. When run, the backdoor component, inst.exe, drops the files explorer.exe, NCHooks.dll, omnithread_rt.dll, and rundll32.exe to the Fonts folder and cygwin1.dll to the System32 folder. It creates the numerous registry entries so that both explorer.exe and rundll32.exe are run automatically on startup. The worm will only run on Windows 2000 and XP operating systems, but the backdoor components will also run on Win9x and Windows NT.

W32/Ganda-A (Aliases: PE_GANDA.A, W32/Ganda@MM, W32/Ganda.A, I-Worm.Ganda, Win32/Ganda.A@mm, W32.Ganda.A@mm, Ganda) (Win32 Worm): This is a worm that spreads by sending itself to e-mail addresses collected from EML, HTM*, DBX, and WAB files on your computer. W32/Ganda-A creates two copies of itself in your Windows folder. One copy is named scandisk.exe; the other is an EXE file with a name consisting of eight randomly chosen lower-case letters. W32/Ganda-A sets the following registry entry so that it loads automatically every time your computer is started:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\ScanDisk = <Windows>\scandisk.exe

While sending e-mails, the worm makes an additional copy of itself in your Windows folder under the name tmpworm.exe. W32/Ganda-A scans through RAM, looking for applications that has any of the following text strings in memory: virus, firewall, F-secure, Symantec, McAfee, PC-Cillin, Trend Micro, Kaspersky, Sophos, or Norton. Processes containing any of the offending strings are terminated. This is intended to kill off a range of popular security products but it can cause collateral damage: for example, if you have a Word document open containing any of the above strings, the worm will shut down Word without giving you a chance to save any changes. W32/Ganda-A infects EXE and SCR files on your hard disk by inserting a small loader program that tries to launch a copy of the worm from your Windows folder when you close the infected application. Files that are modified in this way rely on the original randomly named worm file being present. If you delete the worm files from your Windows folder, then you will immediately make any modified EXE files uninfectious. The worm can send e-mails with several subject line and message text combinations, both in English and Swedish. In all of these cases, the attached file has a random 2-character name and an SCR extension (e.g. oc.scr). The worm also creates entries in the following registry keys:

- HKLM\Software\SS\Sent
- HKLM\Software\SS\Sent2

W32/Ganda-A sends a rambling diatribe complaining about the Swedish education system to a small set of e-mail addresses apparently belonging to Swedish journalists. These e-mails do not contain the worm as an attachment.

W32.HLLW.Begbie@mm (Win32 Worm): This is a worm that attempts to spread through e-mail, KaZaA, and IRC. It uses Microsoft Outlook to e-mail itself to all the contacts in the Windows Address Book. The e-mail message has a randomly chosen subject, message, and attachment, which will have either a .exe or .zip file extension. When W32.HLLW.Begbie@mm is run, it will display a message stating, "This update does not need to be installed on this system." This threat is written in Microsoft Visual Basic (VB). The VB run-time libraries must been installed on the computer to execute.

W32.HLLW.Deborms.B (Alias: Worm.Win32.Deborm.e) (Win32 Worm): This is a worm that attempts to spread through a local network. The worm attempts to connect to port 139 (NetBIOS).

W32.HLLW.Ducktest (Alias: W32/DuckTest.worm) (Win32 Worm): This is a worm that spreads itself to all the network drives and shares. When run, this worm will display a message if the filename is WinQak32.exe. It is possible that the network copy routine may result in garbage being printed by networked printers.

W32.HLLW.Genky (Win32 Worm): This is a worm that spreads using the KaZaA and iMesh file-sharing networks. It also attempts to download Backdoor.Sdbot from a specific web site. It is written in Microsoft Visual Basic, version 6, and packed with FSG.

W32.HLLW.Knon@mm (Win32 Worm): This is a worm that uses Microsoft Outlook and mIRC to spread. It deletes or overwrites many files. The worm is written in Microsoft Visual Basic, version 6.

W32.HLLW.Lovgate.F@mm (Win32 Worm): This is a minor variant of W32.HLLW.Lovgate.C@mm. The only functional difference between this variant and W32.HLLW.Lovgate.C@mm is that W32.HLLW.Lovgate.F@mm will not send any e-mail messages to a malicious user.

W32.HLLW.Nebiwo (Win32 Worm): This is a worm that attempts to connect to your computer using TCP port 445. If successful, the worm copies itself to a set of paths that are hard-coded into the worm, so that it runs when you start Windows. W32.HLLW.Nebiwo also drops Trojans, such as Backdoor.Sdbot, Backdoor.Litmus (2), and Trojan.KillAV. The worm is written in Microsoft Visual C++ and is packed with UPX or ASPack.

W32.HLLW.Oror.AI@mm (Aliases: W32.HLLW.Oror.AD@mm, W32/Roro.AD@mm, I-Worm.Roron.gen) (Win32 Worm): This is a variant of the W32.HLLW.Oror@mm mass-mailing worm. It attempts to spread using e-mail, mIRC, KaZaA, network shares, and mapped drives. The e-mail attachment arrives with a .exe or .scr file extension. W32.HLLW.Oror.AI@mm also attempts to terminate and remove various security products from the infected computer. This threat is written in the C++ language. Some of the files are compressed with UPX.

W32.HLLW.Primcol (Win32 Worm): This is a worm that copies itself to every directory on your hard drive. The worm also deletes the system files if the date is later than July 2. It is a worm written in Visual Basic.

W32.HLLP.Systemp (Win32 Virus): This is a parasitic virus written in C++ (a high-level language), using the MFC libraries. Once W32.HLLP.Systemp is executed, it will insert a backdoor on the user's system.

W32/Hybris-H (Aliases: W32/Hybris.gen@MM, W95.Hybris.worm) (Win32 Worm): This is an e-mail worm which is functionally similar to W32/Hybris-C. The worm drops various plugins in the Windows system folder which determine the worm's specific functionality, e.g. the characteristics of the e-mail messages.

W32/Nicehello-A (Aliases: I-Worm.Nicehello, Win32/NiceDay.A, W32.Nicehello@mm, W32/Nicehello@MM, WORM_NICEHELLO.A, Win32.Rivas.A worm) (Win32 Worm): This is a worm that arrives in an e-mail with various subject lines, message text, and attached files. When the worm is first run, a copy is intended to be created in the folder C:\Windows\system or C:\winnt\system32 with the filename sys64dvr.exe. A bug will cause the worm to be copied to C:\Windows\systemsys64dvr.exe or C:\winnt\system32sys64dvr instead. The following registry entry will be created to run the worm when Windows starts up:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\System 64 Driver for Games = sys64dvr.exe

Since the worm is not copied to the correct location, the worm will not be run when Windows starts up. W32/Nicehello-A sends an e-mail to the malicious user with details of the victim's MSN account. It displays a message box containing the text "Microsoft Windows XP or greater required!"

W32/Oror-T (Aliases: I-Worm/Roron.51, W32/Oror.gen.a@MM) (Win32 Worm): This is a variant of the W32/Oror family of Internet worms which spreads via network shares, file sharing on KaZaA networks and by e-mailing itself to addresses found within files on the local hard drive. The e-mail subject line, message text and attachment filename are randomly chosen from a variety of possibilities. The worm attempts to exploit a known vulnerability in Internet Explorer versions 5.01 and 5.5, so that the attachment is launched automatically when the e-mail is selected for viewing. To prevent reinfection, users of Microsoft Outlook and Outlook Express should install the following patch available from Microsoft: http://www.microsoft.com/technet/security/bulletin/MS01-027.asp. This patch fixes a number of vulnerabilities in Microsoft's software, including the one exploited by this worm.

W32.Spinac@mm (Win32 Worm): This is a worm that uses Microsoft Outlook to spread itself. The e-mail arrives with the following characteristics:

- Subject: <recipient's name>."REMEMBER THE TIMES !!!?
- Attachment: Popey.scr

When W32.Spinac@mm is executed, it may display fake error messages titled, "POPEYE SCREEN SAVER" and "Popeye ScreenMates." The worm is written in Microsoft Visual Basic.

W32.Vote.D@mm (Alias: W32.HLLW.Der@mm) (Win32 Worm): This is a mass mailing worm that attempts to use Microsoft Outlook to e-mail itself to all the contacts in the Windows Address Book. It also attempts to overwrite and delete numerous files on the infected system. The e-mail has the following characteristics:

- Subject: <Recipients.name>, WORLD TRADE CENTER PICTURES
- Attachment: WTC32.scr

This threat is written in Microsoft Visual Basic (VB). The VB run-time libraries must be installed for the worm to execute.

W32/Yaha-R (Win32 Worm): This is a worm from the Yaha family. W32/Yaha-R shares many of the characteristics of W32/Yaha-P. However, W32/Yaha-R stores itself on your hard disk under different file names than those used by the -P variant. W32/Yaha-R places the files wintask32.exe and exeloader.exe into your system folder.

W32.Zokrim.C@mm (Win32 Worm): This is a mass-mailing worm that uses Microsoft Outlook to send itself to all the contacts in the Outlook Address Book. When this worm is run, it displays the message, "Inside error of the program," followed by "Click on my photo." The e-mail has the following characteristics:

- Subject: Your friend Morena
- Attachment: morena.exe

W32.Zokrim.C@mm is written in the Microsoft Visual Basic programming language.

W97M.Saver.C (Word 97 Macro Virus): This is a macro virus that attempts to infect the Normal.dot template and the currently active document when an infected document is opened. It creates an infected document in the Word directory with the name Destrib.dll.

W97M.Timret (Word 97 Macro Virus): This is a macro virus that infects documents when they are opened. It also attempts to send a copy of the infected document through mIRC.

WORM_AXATAK.A (Aliases: W32.HLLW.Axata, W32\AXATAK.worm) (Win32 Worm): Upon execution, this worm copies itself using a random file name in the Windows System folder. It modifies the registry so that its dropped file executes at startup. It also copies itself in the drive C:\ of the infected system. While in memory, it checks the system for mapped network drives with write permission. When it finds one, it copies itself to a random file name in that directory. The worm also copies itself to writable disks in the Floppy Drive of an infected system. The worm runs on Windows 95, 98, ME, NT, 2000, and XP.

WORM_BIBROG.C (Aliases: Win32/Bibrog.C@mm, I-Worm.Academia) Win32 Worm): This memory-resident worm disguises itself as a game where the user shoots a moving image. It uses Microsoft Outlook's Messaging Application Programming Interface (MAPI) to send copies of itself to all recipients found in the Outlook address book. The e-mail message that it sends out has the following characteristics:

- Subject: Fwd: La Academia Azteca
- Attachment: academia.exe

This worm also propagates via KaZaA and other popular peer-to-peer file sharing networks. It drops copies of itself in the following shared folders of KaZaA, ICQ, Grokster, and Morpheus:

- KaZaa\My shared Folder
- ICQ\Shared
- Grokster\My Grokster
- Morpheus\My Shared Folder

This makes its copies readily available for download by other users.

WORM_BIBROG.D (Alias: W32/Bibrog.d@MM) (Win32 Worm): This memory-resident variant of WORM_BIBROG.C appears as a game where a user shoots a moving image. It uses Microsoft Outlook's Messaging Application Programming Interface (MAPI) to send copies of itself to all recipients listed in the Outlook address book. It has the same e-mail message characteristics and propagates the same way that WORM_BIGROG.C does. When executed at startup, this worm also deletes files with the following extensions in all folders: DBF, DLL, EXE, GIF, HML, JPG, MP3, MPG, and ZIP.

WORM_HOLAR.D (Aliases: W32.Hawawi.Worm, W32/Holar.d@MM, I-Worm.Hawawi) (Win32 Worm): This worm propagates via e-mail and via peer-to-peer file-sharing networks, such as KaZaA. It sends e-mail with varying subjects and message bodies and a file attachment that is usually a file named Hawawi.pif. This worm, which runs on Windows 95, 98, ME, NT, 2000, and XP, delivers a destructive payload. It modifies files with certain extensions, leaving these files empty as zero-byte files and non-functional.

WORM_HOLAR.E (Aliases: W32.Hawawi.Worm, W32/Holar.e@MM) (Win32 Worm): This worm is actually an updated version of WORM_HOLAR.D. It drops several files including copies of the D variant. It is destructive and intends to propagate via e-mail and the peer-to-peer file sharing application of KaZaA. The worm uses Microsoft Outlook to send e-mail with varying subjects and message bodies. It looks for target recipients from cached Web pages and HTML files. This worm has a destructive routine of deleting the contents of files with the various extensions. This worm runs on Windows 95, 98, NT, 2000, ME, and XP.

Worm/SMachine.IRC (IRC Worm): This is an Internet worm that spreads through the use of the mIRC network. If executed, the worm creates numerous new files on the C drive. Additionally, so that it gets run each time a user restart their computer the following file gets modified:

- C:\Windows\Win.ini
  load=
  load=C:\Windows\Inf\Inf\System.exe, C:\Windows\Inf\Inf\System.exe

The following registry keys will also get added:

- HKEY_CLASSES_ROOT\CLSID\{D5DE8D20-5BB8-11D1-A1E3-00A0C90F2731}\InProcServer32
  @="C:\\WINDOWS\\INF\\INF\\MSVBVM60.DLL"
  "ThreadingModel"="Apartment"
- HKEY_CLASSES_ROOT\TypeLib\{000204EF-0000-0000-C000-000000000046}\6.0\9\win32
  @="C:\\WINDOWS\\INF\\INF\\MSVBVM60.DLL"
- HKEY_LOCAL_MACHINE\Software\CLASSES\irc\Shell\open\command
  @="\"C:\\WINDOWS\\INF\\INF\\MIRC.EXE\" -noconnect"

WORM_WANOR.A (Alias: W32.HLLW.Wanor@mm) (Win32 Worm): This worm propagates via e-mail using Microsoft Outlook's Messaging Application Programming Interface or MAPI. It sends out an e-mail message with itself as attachment to all addresses listed in the Microsoft Outlook address book. The message has the following characteristics:

- Subject: SAY NOT WAR
- Attachment: Winscr.scr

This worm was designed to drop copies of itself in shared folders of popular peer-to-peer file sharing applications, such as eDonkey2000, KaZaA, Morpheus, Grokster, Bearshare, and ICQ. However, it fails to execute this peer-to-peer propagation routine. If this worm has run at least 20 times, it hides the desktop icons and the Start menu. It then displays an anti-war message with the following text:

- NOT WAR: NOT BLOOD FOR …NOT WAR, SAY NOT WAR

It also continuously blinks the Num Lock LED indicator.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table includes Trojans discussed in the last six months, with new items added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. Note: At times, Trojans may contain names or content that may be considered offensive.

Trojan	Version	CyberNotes Issue #
AdwareDropper-A	A	CyberNotes-2003-04
Backdoor.Acidoor	N/A	CyberNotes-2003-05
Backdoor.Amitis	N/A	CyberNotes-2003-01
Backdoor.Assasin.D	D	CyberNotes-2003-01
Backdoor.Assasin.E	E	CyberNotes-2003-04
Backdoor.Beasty	N/A	CyberNotes-2003-02
Backdoor.Beasty.B	B	CyberNotes-2003-03
Backdoor.Beasty.C	C	CyberNotes-2003-05
Backdoor.Beasty.D	**D**	**Current Issue**
Backdoor.Beasty.E	**E**	**Current Issue**
Backdoor.Bmbot	N/A	CyberNotes-2003-04
Backdoor.Bridco	**N/A**	**Current Issue**
Backdoor.CHCP	N/A	CyberNotes-2003-03
Backdoor.Colfuser	N/A	CyberNotes-2003-01
Backdoor.Cow	N/A	CyberNotes-2003-01
Backdoor.Cybspy	N/A	CyberNotes-2003-01
Backdoor.Dani	N/A	CyberNotes-2003-04
Backdoor.Darmenu	N/A	CyberNotes-2003-05
Backdoor.Deftcode	N/A	CyberNotes-2003-01
Backdoor.Drator	N/A	CyberNotes-2003-01
Backdoor.Dvldr	**N/A**	**Current Issue**
Backdoor.FTP.Casus	N/A	CyberNotes-2003-02
Backdoor.HackDefender	**N/A**	**Current Issue**
Backdoor.Hethat	N/A	CyberNotes-2003-01
Backdoor.Hipo	N/A	CyberNotes-2003-04
Backdoor.Hitcap	N/A	CyberNotes-2003-04
Backdoor.Hornet	N/A	CyberNotes-2003-01
Backdoor.IRC.Aladinz	N/A	CyberNotes-2003-02
Backdoor.IRC.Cloner	N/A	CyberNotes-2003-04
Backdoor.IRC.Yoink	N/A	CyberNotes-2003-05
Backdoor.IRC.Zcrew	N/A	CyberNotes-2003-04
Backdoor.Khaos	N/A	CyberNotes-2003-04
Backdoor.Kilo	N/A	CyberNotes-2003-04
Backdoor.Kol	**N/A**	**Current Issue**
Backdoor.Krei	N/A	CyberNotes-2003-03
Backdoor.Lala	N/A	CyberNotes-2003-01
Backdoor.LittleWitch.C	**C**	**Current Issue**
Backdoor.Longnu	**N/A**	**Current Issue**

Trojan	Version	CyberNotes Issue #
Backdoor.Marotob	**N/A**	**Current Issue**
Backdoor.Massaker	N/A	CyberNotes-2003-02
Backdoor.MSNCorrupt	**N/A**	**Current Issue**
Backdoor.NetDevil.B	B	CyberNotes-2003-01
Backdoor.NetTrojan	N/A	CyberNotes-2003-01
Backdoor.Ohpass	N/A	CyberNotes-2003-01
Backdoor.OICQSer.165	N/A	CyberNotes-2003-01
Backdoor.OICQSer.17	17	CyberNotes-2003-01
Backdoor.Optix.04.d	04.d	CyberNotes-2003-04
Backdoor.OptixPro.10.c	10.c	CyberNotes-2003-01
Backdoor.Plux	N/A	CyberNotes-2003-05
Backdoor.PSpider.310	310	CyberNotes-2003-05
Backdoor.Queen	**N/A**	**Current Issue**
Backdoor.Redkod	N/A	CyberNotes-2003-05
Backdoor.Remohak.16	16	CyberNotes-2003-01
Backdoor.RemoteSOB	N/A	CyberNotes-2003-01
Backdoor.Rephlex	N/A	CyberNotes-2003-01
Backdoor.SchoolBus.B	B	CyberNotes-2003-04
Backdoor.Sdbot.C	C	CyberNotes-2003-02
Backdoor.Sdbot.D	D	CyberNotes-2003-03
Backdoor.Sdbot.E	**E**	**Current Issue**
Backdoor.Serpa	N/A	CyberNotes-2003-03
Backdoor.Servsax	N/A	CyberNotes-2003-01
Backdoor.SilverFTP	N/A	CyberNotes-2003-04
Backdoor.Sixca	N/A	CyberNotes-2003-01
Backdoor.Snowdoor	N/A	CyberNotes-2003-04
Backdoor.Socksbot	**N/A**	**Current Issue**
Backdoor.SubSari.15	15	CyberNotes-2003-05
Backdoor.SubSeven.2.15	2.15	CyberNotes-2003-05
Backdoor.SysXXX	**N/A**	**Current Issue**
Backdoor.Talex	N/A	CyberNotes-2003-02
Backdoor.Udps.10	10	CyberNotes-2003-03
Backdoor.Unifida	N/A	CyberNotes-2003-05
Backdoor.Upfudoor	N/A	CyberNotes-2003-01
Backdoor.VagrNocker	N/A	CyberNotes-2003-01
Backdoor.Vmz	N/A	CyberNotes-2003-01
Backdoor.Xenozbot	N/A	CyberNotes-2003-01
Backdoor.Xeory	N/A	CyberNotes-2003-03
Backdoor.Zdemon	N/A	CyberNotes-2003-02
Backdoor.Zdown	N/A	CyberNotes-2003-05
Backdoor.Zix	N/A	CyberNotes-2003-02
Backdoor.Zvrop	N/A	CyberNotes-2003-03
Backdoor-AFC	N/A	CyberNotes-2003-05
Backdoor-AOK	N/A	CyberNotes-2003-01
BackDoor-AQL	N/A	CyberNotes-2003-05
BackDoor-AQT	N/A	CyberNotes-2003-05
BackDoor-ARR	**ARR**	**Current Issue**
Backdoor-ARU	**ARU**	**Current Issue**

Trojan	Version	CyberNotes Issue #
BackDoor-ARX	**ARX**	**Current Issue**
BackDoor-ARY	**ARY**	**Current Issue**
BDS/AntiPC	N/A	CyberNotes-2003-02
BDS/Backstab	N/A	CyberNotes-2003-02
BDS/Evolut	N/A	CyberNotes-2003-03
Daysun	**N/A**	**Current Issue**
DoS-iFrameNet	N/A	CyberNotes-2003-04
Downloader-BO.dr.b	N/A	CyberNotes-2003-02
Downloader-BS	N/A	CyberNotes-2003-02
Downloader-BW	N/A	CyberNotes-2003-05
Downloader-BW.b	**BW.b**	**Current Issue**
Exploit-IISInjector	N/A	CyberNotes-2003-03
Hacktool.PWS.QQPass	**N/A**	**Current Issue**
ICQPager-J	N/A	CyberNotes-2003-05
IRC/Backdoor.e	E	CyberNotes-2003-01
IRC/Backdoor.f	f	CyberNotes-2003-02
IRC/Backdoor.g	g	CyberNotes-2003-03
IRC/Flood.ap	N/A	CyberNotes-2003-05
IRC/Flood.bi	N/A	CyberNotes-2003-03
IRC/Flood.br	**br**	**Current Issue**
IRC-Emoz	N/A	CyberNotes-2003-03
IRC-OhShootBot	N/A	CyberNotes-2003-01
JS.Fortnight.B	**B**	**Current Issue**
JS.Seeker.J	J	CyberNotes-2003-01
JS/Seeker-C	C	CyberNotes-2003-04
JS_WEBLOG.A	A	CyberNotes-2003-05
KeyLog-Kerlib	N/A	CyberNotes-2003-05
Keylog-Razytimer	N/A	CyberNotes-2003-03
KeyLog-TweakPan	N/A	CyberNotes-2003-02
Linux/Exploit-SendMail	N/A	CyberNotes-2003-05
MultiDropper-FD	N/A	CyberNotes-2003-01
Pac	N/A	CyberNotes-2003-04
ProcKill-AE	N/A	CyberNotes-2003-05
ProcKill-AF	N/A	CyberNotes-2003-05
ProcKill-Z	N/A	CyberNotes-2003-03
PWS-Aileen	N/A	CyberNotes-2003-04
PWSteal.AlLight	N/A	CyberNotes-2003-01
PWSteal.Rimd	N/A	CyberNotes-2003-01
PWSteal.Senhas	N/A	CyberNotes-2003-03
PWS-Tenbot	N/A	CyberNotes-2003-01
QDel359	N/A	CyberNotes-2003-01
QDel373	**1373**	**Current Issue**
Qdel374	**1374**	**Current Issue**
Qdel375	**1375**	**Current Issue**
Renamer.c	N/A	CyberNotes-2003-03
StartPage-G	**G**	**Current Issue**
Stoplete	**N/A**	**Current Issue**
Tellafriend.Trojan	N/A	CyberNotes-2003-04

Trojan	Version	CyberNotes Issue #
TR/Fake.YaHoMe.1	N/A	CyberNotes-2003-02
Tr/SpBit.A	A	CyberNotes-2003-04
TR/WinMx	N/A	CyberNotes-2003-02
Troj/Dloader-BO	N/A	CyberNotes-2003-02
Troj/Manifest-A	N/A	CyberNotes-2003-03
Troj/Qzap-248	N/A	CyberNotes-2003-01
Troj/SadHound-A	N/A	CyberNotes-2003-03
Troj/Slacker-A	A	CyberNotes-2003-05
Troj/Slanret-A	N/A	CyberNotes-2003-03
Troj/TKBot-A	A	CyberNotes-2003-04
TROJ_JBELLZ.A	A	CyberNotes-2003-02
TROJ_KILLBOOT.B	B	CyberNotes-2003-01
TROJ_RACKUM.A	A	CyberNotes-2003-05
Trojan.Barjac	N/A	CyberNotes-2003-05
Trojan.Dasmin	N/A	CyberNotes-2003-01
Trojan.Dasmin.B	B	CyberNotes-2003-03
Trojan.Downloader.Aphe	**N/A**	**Current Issue**
Trojan.Downloader.Inor	N/A	CyberNotes-2003-02
Trojan.Grepage	N/A	CyberNotes-2003-05
Trojan.Idly	N/A	CyberNotes-2003-04
Trojan.Ivanet	N/A	CyberNotes-2003-02
Trojan.KKiller	N/A	CyberNotes-2003-01
Trojan.Poldo.B	B	CyberNotes-2003-02
Trojan.Poot	N/A	CyberNotes-2003-05
Trojan.ProteBoy	N/A	CyberNotes-2003-04
Trojan.PSW.Gip	**N/A**	**Current Issue**
Trojan.PSW.Platan.5.A	N/A	CyberNotes-2003-01
Trojan.PWS.QQPass.D	N/A	CyberNotes-2003-02
Trojan.Qforager	N/A	CyberNotes-2003-02
Trojan.Qforager.Dr	N/A	CyberNotes-2003-02
Trojan.Qwe	N/A	CyberNotes-2003-02
Trojan.Snag	N/A	CyberNotes-2003-02
Trojan.Unblockee	N/A	CyberNotes-2003-01
Uploader-D	**D**	**Current Issue**
VBS.Kasnar	**N/A**	**Current Issue**
VBS.Moon.B	B	CyberNotes-2003-02
VBS.StartPage	N/A	CyberNotes-2003-02
VBS.Trojan.Lovcx	N/A	CyberNotes-2003-05
VBS/Fourcourse	**N/A**	**Current Issue**
W32.Benpao.Trojan	N/A	CyberNotes-2003-04
W32.CVIH.Trojan	**N/A**	**Current Issue**
W32.Socay.Worm	N/A	CyberNotes-2003-02
W32.Systentry.Trojan	N/A	CyberNotes-2003-03
W32.Xilon.Trojan	N/A	CyberNotes-2003-01
W32.Yinker.Trojan	N/A	CyberNotes-2003-04
W32/Igloo-15	N/A	CyberNotes-2003-04
Xin	N/A	CyberNotes-2003-03

BackDoor-ARR (Alias: Backdoor.GrayBird): This Trojan uses an icon that would appear to the victim to be a legitimate setup program for Norton Anti-Virus. Once the server component of this Trojan is run on the victim machine, the malicious user is able to connect to and administer that machine. When run, the Trojan installs itself onto the system, copying itself to the System directory. It creates the following registry keys in order to run at Windows start up:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "winlogon" = %SysDir%\SVCH0ST.EXE
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices "winlogon" = %SysDir%\SVCH0ST.EXE
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "winlogon" = %SysDir%\SVCH0ST.EXE

It also creates the following entry in the WIN.INI file in order to run at Windows start up, "run=%SysDir%\SVCH0ST.EXE." The Trojan allows numerous actions to be performed on the victim machine.

Backdoor-ARU (Alias: Backdoor.Skubur): This remote access Trojan allows a malicious user to connect to an infected system on TCP port 1354 to perform various functions. When run, the Trojan creates a registry run key to load itself at system startup:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ Run "skullburrow" = %Trojan Path%

Once the computer has become compromised it can allow the malicious user to:

- Steal computer information (username, password, ip-address etc.)
- Upload/download/rename/delete/etc files on the infected system)

BackDoor-ARX: This remote access Trojan allows a malicious user to connect to an infected system on TCP port 3000 to perform various functions. When run, the Trojan creates a registry run key to load itself at system startup:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ Run "dllService" = %Trojan Path%

The Trojan has various functionalities:

- ICQ client (allows Trojan to "talk" to ICQ servers)
- FTP server (allows Trojan to upload/download/rename/delete/etc files on the infected system)
- Proxy server (allows the Trojan to relay network traffic)

BackDoor-ARY: This is a backdoor Trojan package, which includes several files with the .scr extension. When run, it opens port 1234, and port 5190 and listens on these ports. The other .scr files are all written in Visual Basic. Most of files have length 20,480 bytes. These files have version information with product name "aolrelay." When run, these files connect to various IRC servers.

Backdoor.Beasty.D: This is a backdoor Trojan that is similar to Backdoor.Beasty, Backdoor.Beasty.B, and Backdoor.Beasty.C. This Trojan is a Delphi application and is packed with UPX, v0.76.1-1.20. It gives a malicious user complete access to your computer. By default, the Trojan listens on port 666 and notifies the malicious user through e-mail or ICQ. The Trojan attempts to terminate various security products and system monitoring tools.

Backdoor.Beasty.E (Alias: Backdoor.Plux): This Trojan opens a listening port on your computer. This action could allow a malicious user to remotely control your computer. It uses web.icq.com to send a message to the malicious user's ICQ Unified Messaging Center. This message includes the IP address of the infected computer.

Backdoor.Bridco: This is a backdoor Trojan that uses MSN Messenger (.NET messenger). This Trojan allows a malicious user to access your computer by stealing an MSN Messenger password and sending messages using the MSN messenger service.

Backdoor.Dvldr (Aliases: Win32.Deloder Trojan, BKDR_DELODER.A), BackDoor.ARG): This is a backdoor Trojan that gives a malicious user unauthorized access to your computer. The worm, W32.HLLW.Deloder, installs this Trojan.

Backdoor.HackDefender: This is a backdoor Trojan component that hides processes, services, and files. The Backdoor.HackDefender package consists of two files:

- Hxdefxxx.exe, which is the backdoor component.
- Hxdefxxx.ini, which is the backdoor configuration file.

When Backdoor.HackDefender is activated, it registers itself as a service, causing the system to execute the backdoor every time you restart the computer and causes the service control manager to create the registry key:

- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\HackerDefenderxxx

This key contains the configuration information, such as its display name, "HXD Service," for the backdoor service. The Trojan inventories all the processes on the system. It injects its own code into their memory and hooks various APIs and waits for you to launch other processes, into which the Trojan will also inject its own code, as well as hook their APIs.

Backdoor.Kol: This is a Backdoor Trojan that gives a malicious user unauthorized access to a compromised computer. The Backdoor is controlled via commands issued by the malicious user through several IRC channels. Backdoor.Kol is a Delphi application, packed with ASPack v2.11. When Backdoor.Kol runs, it copies itself as one of the following randomly chosen file names:

- %Windir%\Loader32.exe
- %Windir%\Mstask32.exe

and creates one of the following randomly chosen registry values so that the Trojan runs when you restart Windows, “Dynamic Link Library loader %windows%\Loader32.exe,” in the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

“Microsoft Task Manager %windows%\mstask32.exe,” in the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

“Windows IP Monitor WinIPM.exe,” in the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

It connects to an IRC server, joins several specific channels, and waits for commands that the malicious user transmits through IRC.

Backdoor.LittleWitch.C (Alias: trojan LittleWitch v6.1): Backdoor.LittleWitch.C: This is a backdoor Trojan that is similar to Backdoor.LittleWitch.B. This Trojan gives a malicious user unauthorized access to a compromised computer. The presence of the file, Rundll.exe, in the %System% folder is an indicator of a possible infection. By default, Backdoor.LittleWitch.C opens both TCP and UDP ports 31320 on the infected computer. It is a Delphi application. Unlike Backdoor.LittleWitch.B, Backdoor.LittleWitch.C is not packed.

Backdoor.Longnu: This is a Trojan that gives a malicious user access to your computer. It downloads other components from specific web sites. Upon execution, this Trojan also displays a fake error message, “Error #251: Failed to init randomized generator." Backdoor.Longnu is written in Microsoft Visual Basic, version 6. When Backdoor.Longnu runs, it displays the fake error message, "Error #251: Failed to init randomize generator."

Backdoor.Marotob: This is a Trojan horse that steals e-mail addresses and other information. It opens TCP port 701 to connect to the malicious user and gives the malicious user unauthorized access to your computer. When Backdoor.Marotob runs, it queries the registry to locate the ICQ installation folder, and if found, retrieves e-mail addresses from the contact list files in that folder. It also queries the registry to locate the Windows Address Book and retrieves e-mail addresses from it and then sends the stolen information to the malicious user.

Backdoor.MSNCorrupt (Aliases: Backdoor.MSNCorrupt, Backdoor.:Win32/MSNCorrupt): This is a backdoor Trojan that uses MSN Messenger to connect to your computer. When Backdoor.MSNCorrupt is executed, it copies itself as C:\Windows \System32\SysOps.exe. This path is hard-coded, so the copy routine will fail if Windows is installed to any other location. It will creates the value, "SysOps SysOps," in the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

The Trojan waits for you to connect to the Internet using MSN Messenger. When you do so, the Trojan sends a notification to the malicious user. Then, the malicious user can send commands to your computer.

Backdoor.Queen: This is a backdoor Trojan that runs only under Windows NT, Windows 2000, and Windows XP. It gives the malicious user unauthorized access to the infected computer. The Trojan attempts to disguise itself as the normal Windows process named "LSASS.EXE." The Trojan has two components:

- QoSServer.dll: the backdoor Trojan
- QoSServer.exe: the loader of Backdoor.Queen

When Backdoor.Queen runs, it creates the automatic start service, "QoSserver," and attempts to create a remote thread in "LSASS.EXE" and inject itself into it. The Trojan listens on port 8491 and waits for commands from the malicious user.

Backdoor.Sdbot.E: This is a backdoor Trojan that is a variant of Backdoor.Sdbot. This variant has been compressed with UPX v0.76.1-1.20. It gives a malicious user unauthorized access to your computer, allowing a malicious user to control it using commands issued through IRC.

Backdoor.Socksbot: This is a backdoor Trojan that connects to IRC and allows a malicious user to control your computer. Backdoor.Socksbot consists of two components:

- Proxyspam.exe
- Socks8080.exe, which is also copied to the computer as Svhost.exe

When Backdoor.Socksbot is executed, it copies itself as:

- %System%\Svhost.exe
- C:\WINNT\System32\Proxyspam.exe
- C:\WINNT\System32\Socks8080.exe, which is a copy of Svhost.exe

and adds the values:

- Svhost Loader Svhost.exe
- Service C:\WINNT\SYSTEM32\SOCKS8080.EXE

to the registry key:

- HKEY\LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

It also ads the value, "Svhost Loader Svhost.exe," to the registry key:

- HKEY\LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

Next it attempts to connect to an IRC server and notify the malicious user.

Backdoor.SysXXX: This is a backdoor Trojan program that was written in the Delphi language. It gives a malicious user complete access to your computer. By default, the Trojan opens two TCP ports, 31556 and 6051, which it uses to communicate with the malicious user. It notifies the malicious user through e-mail or ICQ. Also, Backdoor.SysXXX attempts to terminate various security products and system monitoring tools.

Daysun: This threat consists of two files, Sunday.exe and Sunday.vbs. These threats are detected as Daysun and VBS/Daysun respectively. On executing the file Sunday.exe, the Trojan will drop the VBScript file Sunday.vbs into the hardcoded directory:

- C:\Windows\System32 and Sunday.exe into windows SYSTEM32 directory.

Daysun will also modify the registry setting:

- Hkey_Current_User\Software\Microsoft\Windows\CurrentVersion\Run "Sunday" "c:\windows\system32\Sunday.vbs"

If day is Sunday, the virus will display a message on startup of the machine and will also modify the registry settings:

- Hkey_Local_Machine\Software\Microsoft\Windows\CurrentVersion\RunServices\DisableKeyboard,Rundll32.exe Keyboard,Disable
- Hkey_Local_Machine\Software\Microsoft\Windows\CurrentVersion\RunServices\DisableMouse,Rundll32.exe Mouse,Disable

Downloader-BW.b (Aliases: Trojan.GreetCard.3072, TrojanDownloader.Win32.Greetyah): This Trojan downloads and installs a remote executable. At the time of writing, the remote file was unavailable rendering this downloader useless. The Trojan bears similarities with a previous variant. The downloader is likely to be received via an e-mail masquerading as a greeting card. The Trojan was spammed out in this manner recently. When the downloader is run on the victim machine, a fake error message is displayed. It then attempts to download a remote executable (unavailable at the time of writing):

- http://view-greetings-yahoo.com/sysman32.exe

The SYSMAN32.EXE file is downloaded to %SysDir% as SYSMAN32.EXE, and a registry key is added to launch it at subsequent system startup. For example:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "SystemManager" = C:\WINNT\System32\sysman32.exe

Hacktool.PWS.QQPass: This is a Trojan creation tool. The Trojans created with this tool can be programmed to steal dial-up networking telephone numbers and passwords, as well as the passwords of OICQ, which is a popular Chinese chat program. The filename of the file detected as Hacktool.PWS.QQPass and consists of five random letters with the .exe extension. Then, the Trojan sends this information to a specified set of e-mail addresses.

IRC/Flood.br: This is an Internet Relay Chat BOT/DDoS tool. It is dropped by a self-extracting archive that generally includes a copy of the mIRC client within itself. This allows users who do not run mIRC to become used in a DDoS attack. When run, the dropper creates a directory and extracts several files to it. If mIRC is already installed on a system, registry entries pointing to the installed product will be redirected to the version dropped by the Trojan. Additionally, a registry entry is created by the dropper to run mIRC at system startup:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "explorer"=%WinDir%\Media\EXPL32.EXE

JS.Fortnight.B: This is a Trojan horse that drops a file that is then inserted into the default Microsoft Outlook Express signature. Then, every time you send e-mail using Outlook Express, the message will contain code attempting to open a specific Web site when the message is opened. JS.Fortnight.B also changes the Internet Explorer security settings. It also configures the Web Browser to prepend all the URLs with a specific URL.

QDel373: This Trojan file is written in Visual Basic 6, and is not internally compressed with a packer, filesize was 28.672 bytes (decimal). Upon running the file, a fake GUI (Graphical User Interface) display box appears and the Trojan has been trying to delete numerous files on the local system. The machine is likely to stop responding at this stage.

Qdel374 (Alias: Trojan.Win32.KillFiles.bc): On execution the Trojan will display a message. The Trojan then proceeds to delete files in:

- C:\winnt*.*
- C:\windows*.*
- C:\winnt\fonts*.*
- C:\windows\fonts*.*

Qdel375: On execution, the Trojan will display a message. The Trojan will save itself as winrar.exe in the Windows directory and will then append 36Bytes of text message"

- Your comp f*cked! I am robof*cker..Your comp f*cked! I am CompF*cker! to IExplore.exe, Excel.exe, Winword.exe, wab.exe and regedit.exe.

The Trojan may reboot the system.

StartPage-G (Alias: Troj/StartPageD): This Trojan is compressed with the UPX packer. When the Trojan is executed, it will modify the Internet Explorer start page setting in the registry:

- Hkey_Current_User\Software\Microsoft\Internet Explorer\Main\Local Page "http://www.q88p.net/09.htm
- Hkey_Current_User\Software\Microsoft\Internet Explorer\Main\Start Page http://www.q88p.net/09.htm

It will also change the registry setting to execute the Trojan on start up of machine:

- Hkey_Local_Machine\Software\Microsoft\CurrentVersion\RunServices\B.B(oZc) "[folder where file saved in]\mouse.exe"

The Trojan will also create the file winweb.ini that contains the startpage changes.

Stoplete: On execution, the Trojan will display a message and if the user clicks the button, the Trojan will disable the mouse and keyboard and display another message. The Trojan will save itself to C:\Windows\Start Menu\Programs\Startup or c:\Winnt\StartMenu\Programs\Startup. The mouse and keyboard will be functional upon reboot of the system.

Trojan.Downloader.Aphe (Aliases: TrojanDownloader.Win32.Aphex.10.d, TrojanDownloader.Win32/Aphex.1_0.D): This is a Trojan horse that attempts to download a file from a specific Web site, and then execute it. When Trojan.Downloader.Aphe is executed, it copies itself as %Windir%\Windows33.exe and adds the value, "windows33 %windir%\windows33.exe," to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

It also attempts to stop the following services:

- NAVAPSVC
- PERSFW
- AVPCC

If the file, %Windir%\Xtb.exe, is not found, the Trojan attempts to download a file from a specified Web site and then execute it.

Trojan.PSW.Gip (Aliases: Trojan.PSW.Gip.113.b, PWS-CK trojan, Troj/Gip-113-B): This is a Trojan horse that tries to steal passwords and may download a file from a specified Web site. Trojan.PSW.Gip also makes many changes to the registry.

Uploader-D: This uploader Trojan may arrive in an e-mail message, which is detected as Exploit-MIME.gen.exe. On an unpatched system, the file will run automatically. This message is not created by the Trojan, but is likely created by the Trojan author and SPAMed to unsuspecting users. Once run, the Trojan searches the victim machine for DOC files to send out to two pre-set e-mail addresses. Using its own SMTP engine, it sends the e-mail through an SMTP server specified within the Trojan executable. Once the Trojan is done, it removes itself from memory. The Trojan also does not copy itself locally, and it does not create entries in the registry or INI files to run again upon startup.

VBS/Fourcourse: This Trojan consists of two script files. When executed, the Trojan file will drop another VBScript named sysw32.vbs into the root directory. It will also modify the following registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\sys32, "C:\sysw32.vbs"

This dropped file will attempt to dial a phone number using the COM ports if the date is before April 1st 2003.

VBS.Kasnar: This is a Trojan horse that creates many garbage text files on the infected computer. When VBS.Kasnar runs, it copies itself as %Windir%\sysops.vbs and adds the value, "MSrundll32 sysops.vbs," to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs when you start Windows. It also modifies the value data of the value RegisteredOwner in the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion

to, "RegisteredOwner DumbaSS." If the current system day is 7, the Trojan displays three messages with the following characteristics:

- Text: This virus is dedicated to the Black Cat Virus Group, you guys rule!
- Text: VBS.Ransak by wHacker...pure annoyance
- Text: Currently spawning 100,000 files in multiple folders and drives, good day!

The Trojan then creates many 116-byte text files in the following folders:

- C:\
- C:\Windows
- C:\Windows\System32
- C:\Program Files\KaZaA\KaZaA Lite\my shared folder
- A:\

The files have numbers as the names and .txt as extension. For example, the file may be named 78.txt.

W32.CVIH.Trojan: This is a Trojan horse. It copies itself to the %System% folder, and then executes the copied file. W32.CVIH.Trojan also attempts to close windows and delete the files of various antivirus and firewall programs.